Journal of Algebra 635 (2023) 790–821

Contents lists available at ScienceDirect

Journal of Algebra

journal homepage: www.elsevier.com/locate/jalgebra

Modular curves with many points over finite fields

Valerio Dose [a,*], Guido Lido [b,1], Pietro Mercuri [c], Claudio Stirpe [d]

[a] *Department of Computer, Control and Management Engineering, "Sapienza" University of Rome, Roma, Italy*
[b] *Department of Mathematics, University of Rome "Tor Vergata", Roma, Italy*
[c] *Dipartimento SBAI, "Sapienza" University of Rome, Roma, Italy*
[d] *Convitto Nazionale "R. Margherita", Anagni, Italy*

A R T I C L E   I N F O

Article history:
Received 26 October 2022
Available online 17 July 2023
Communicated by Kirsten Eisenträger

MSC:
11G20
11G18
14G35

Keywords:
Many points
Finite fields
Modular curves
Chen's isogeny
Cartan subgroups
Hecke operators

A B S T R A C T

We describe an algorithm to compute the number of points over finite fields on a broad class of modular curves: we consider quotients X_H/W for H a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ such that for each prime p dividing n, the subgroup H at p is either a Borel subgroup, a Cartan subgroup, or the normalizer of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})$, and for W any subgroup of the Atkin-Lehner involutions of X_H. We applied our algorithm to more than ten thousand curves of genus up to 50, finding more than one hundred record-breaking curves, namely curves $X/\mathbb{F}_q$ with genus g that improve the previously known lower bound for the maximum number of points over $\mathbb{F}_q$ of a curve with genus g. As a key technical tool for our computations, we prove the generalization of Chen's isogeny to all the Cartan modular curves of composite level.

* Corresponding author.
E-mail addresses: valerio.dose@uniroma1.it (V. Dose), guidomaria.lido@gmail.com (G. Lido), mercuri.ptr@gmail.com (P. Mercuri), clast@inwind.it (C. Stirpe).

[1] The second author is supported by the MIUR Excellence Department Project MatMod@TOV awarded to the Department of Mathematics, University of Rome Tor Vergata, by the "Programma Operativo Nazionale (PON) "Ricerca e Innovazione" 2014-2020" and by the "National Group for Algebraic and Geometric Structures, and their Applications" (GNSAGA - INdAM).

https://doi.org/10.1016/j.jalgebra.2023.07.013
0021-8693/

1. Introduction

Finding among the algebraic curves of a fixed genus, the ones with the largest number of points over a finite field of fixed cardinality, is an interesting effort in algebraic geometry and number theory which also has applications in coding theory (see for example [27, Section 8.4]). The Weil bound prescribes the inequality

$$\#C(\mathbb{F}_q) \leqslant q + 1 + 2g\sqrt{q},$$

where $\#C(\mathbb{F}_q)$ is the number of points over a finite field $\mathbb{F}_q$, with q being a prime power, of a nonsingular, projective, absolutely irreducible curve C of genus g.

Let q be a fixed prime power. As it is shown in [29] and [31], the previous estimate cannot be sharp for g large since

$$N_g(\mathbb{F}_q) \leqslant g(\sqrt{q} - 1) + o(g), \quad \text{for } g \to +\infty,$$

where $N_g(\mathbb{F}_q) := \max_{C \text{ of genus } g} \#C(\mathbb{F}_q)$. Several sequences $\{C_n\}_{n \in \mathbb{N}}$ of algebraic curves over $\mathbb{F}_q$ with increasing genus g_n, have been found to achieve the asymptotic bound $\lim_{n \to +\infty} \dfrac{\#C_n(\mathbb{F}_q)}{g_n} = \sqrt{q} - 1$. Among these sequences, one of the most classical example is obtained by taking modular curves $X_0(m)$ with certain increasing levels m and counting supersingular points over a field $\mathbb{F}_q$, where q is a square, see [28]. Concerning curves with small genus, the website [30] is devoted to collect the full list of known upper bounds $M_g(\mathbb{F}_q)$ and lower bounds $L_g(\mathbb{F}_q)$ for $N_g(\mathbb{F}_q)$, when $g \leqslant 50$ and for fields of characteristic less than 100 with small cardinality. Notice that $M_g(\mathbb{F}_q)$ and $L_g(\mathbb{F}_q)$ depend on the current state of the art in this line of research.

In this paper we look at this question concentrating on a large class of modular curves. Namely, we consider modular curves X_H associated to a subgroup H of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ such that, for each prime p dividing n, with maximum power e, the reduction of H modulo p^e is either a Borel subgroup, a Cartan subgroup, or the normalizer of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})$. We also consider quotients of these curves by Atkin-Lehner involutions w_p whenever H is a Borel subgroup at p. We give an algorithm which computes the number of points over a finite field on these modular curves, without having the equation of the curve, but only using the trace of Hecke operators acting on modular abelian varieties associated to weight 2 newforms invariant under the congruence subgroup $\Gamma_0(m)$. Numerical approximations of these traces can be computed with the methods described in [3] and they have been collected for $m \leqslant 10000$ in the database available at [18].

We applied our algorithm to these modular curves over small finite fields of characteristic less than 20 using data available on [18]. Furthermore, in September 2022 we compared our results with the best known curves available on the database [30] and we found many improvements that we list in the final section of this paper.

To make the computation, we prove that the Jacobian of the modular curves X_H we are considering, are isogenous to a product of modular abelian varieties associated to weight 2 newforms invariant under the congruence subgroup $\Gamma_0(m)$. We give explicitly this factorization of the Jacobian (Theorem 3.8), generalizing results of [8], [15], [9], [11].

The idea to use these types of modular curves builds on recent work on computing equations, rational points, and automorphism groups for such curves, as for example [19], [23], [12], [11], [13], [10], [22], [4], [5], [16], [1]. Another algorithm has been recently devised for computing the number of points on X_H for a general H, see [26, Section 5]. Their method does not make use of the factorization of the Jacobian of the modular curve up to isogeny, but they rather can obtain it case by case as a consequence of the computation of the number of points of the curves over many fields of different characteristic [26, Section 6].

The paper is organized as follows. In Section 2 we introduce the definitions related to the modular curves we are considering. In Section 3 we describe the Jacobians of our curves, up to isogeny, explicitly in terms of the Jacobian of Borel modular curves. In Section 4 we discuss the algorithm we use to compute the number of points over finite fields.

In Section 5 we give asymptotic results to estimate the number of $\mathbb{F}_q$-points on our curves when the genus g is large. Finally, in Section 6 and in the Appendix, we collect the results obtained. In particular, for every choice of g and $\mathbb{F}_q$, we list in the Appendix the curve with the largest number of points among the ones we considered, and in Section 6, for the convenience of the reader, we collect all the examples which improve the previously known lower bounds $L_g(\mathbb{F}_q)$.

2. Modular curves of mixed type

Let n be a positive integer. For each subgroup H of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ with surjective determinant, we define

$$\Gamma_H := \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma^T \pmod{n} \text{ lies in } H\}.$$

Let $\mathbb{H} = \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}$ be the complex upper half-plane and denote by $\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ the extended complex upper half-plane. We define the modular curve associated to H:

$$X_H := \Gamma_H \backslash \mathbb{H}^*.$$

For a more detailed reference about this construction see [11, Section 1]. In the following, we choose a non-square element $\xi \in (\mathbb{Z}/p^e\mathbb{Z})^\times$ when p is an odd prime and e is a positive integer. We define the following subgroups of $\mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})$ for every prime p:

$$B^0(p^e) := \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix}, a, c, d \in \mathbb{Z}/p^e\mathbb{Z}, \quad ad \not\equiv 0 \bmod p \right\};$$

$$C_{\mathrm{s}}(p^e) := \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}, a, d \in (\mathbb{Z}/p^e\mathbb{Z})^\times \right\};$$

$$C_{\mathrm{s}}^{+}(p^e) := C_{\mathrm{s}}(p^e) \cup \left\{ \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}, b, c \in (\mathbb{Z}/p^e\mathbb{Z})^{\times} \right\};$$

$$C_{\mathrm{ns}}(2^e) := \left\{ \begin{pmatrix} a & b \\ b & a+b \end{pmatrix}, a, b \in \mathbb{Z}/2^e\mathbb{Z}, (a,b) \not\equiv (0,0) \bmod 2 \right\};$$

$$C_{\mathrm{ns}}^{+}(2^e) := C_{\mathrm{ns}}(2^e) \cup \left\{ \begin{pmatrix} a & a-b \\ b & -a \end{pmatrix}, a, b \in \mathbb{Z}/2^e\mathbb{Z}, (a,b) \not\equiv (0,0) \bmod 2 \right\};$$

$$C_{\mathrm{ns}}(p^e) := \left\{ \begin{pmatrix} a & b\xi \\ b & a \end{pmatrix}, a, b \in \mathbb{Z}/p^e\mathbb{Z}, (a,b) \not\equiv (0,0) \bmod p \right\}, \quad \text{if } p \text{ is odd;}$$

$$C_{\mathrm{ns}}^{+}(p^e) := C_{\mathrm{ns}}(p^e) \cup \left\{ \begin{pmatrix} a & b\xi \\ -b & -a \end{pmatrix}, a, b \in \mathbb{Z}/p^e\mathbb{Z}, (a,b) \not\equiv (0,0) \bmod p \right\}, \quad \text{if } p \text{ is odd;}$$

$$B_r(p^e) := \left\{ \begin{pmatrix} a & bp^r \\ cp^{r+1} & d \end{pmatrix}, a, b, c, d \in \mathbb{Z}/p^e\mathbb{Z}, \quad ad \not\equiv 0 \bmod p \right\},$$

for $r = 0, 1, \ldots, e-1$;

$$T_r(p^e) := \left\{ \begin{pmatrix} a & bp^r \\ cp^r & d \end{pmatrix}, a, b, c, d \in \mathbb{Z}/p^e\mathbb{Z}, ad - bcp^{2r} \in (\mathbb{Z}/p^e\mathbb{Z})^{\times} \right\}.$$

We remark that $T_e(p^e) = C_{\mathrm{s}}(p^e)$ and that $C_{\mathrm{s}}(p^e), C_{\mathrm{ns}}(p^e)$ are respectively a split and a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})$ and, with the exception of $C_{\mathrm{s}}^{+}(2^e)$, the groups $C_{\mathrm{s}}^{+}(p^e), C_{\mathrm{ns}}^{+}(p^e)$ are the corresponding normalizers inside $\mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})$.

Given n_0, n_{0^+}, n_{s}, n_{s^+}, n_{ns}, n_{ns^+} pairwise coprime positive integers such that $n = n_0 n_{0^+} n_{\mathrm{s}} n_{\mathrm{s}^+} n_{\mathrm{ns}} n_{\mathrm{ns}^+}$. By Chinese Remainder Theorem we have $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \cong \prod_{i=1}^{r} \mathrm{GL}_2(\mathbb{Z}/p_i^{e_i}\mathbb{Z})$. We look at the subgroups of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ of the following form

$$H \cong \prod_{i=1}^{r} H_{p_i}, \quad \text{where } H_{p_i} = \begin{cases} B^0(p_i^{e_i}), & \text{if } p_i \mid n_0 n_{0^+}, \\ C_{\mathrm{s}}(p_i^{e_i}), & \text{if } p_i \mid n_{\mathrm{s}}, \\ C_{\mathrm{s}}^{+}(p_i^{e_i}), & \text{if } p_i \mid n_{\mathrm{s}}^{+}, \\ C_{\mathrm{ns}}(p_i^{e_i}), & \text{if } p_i \mid n_{\mathrm{ns}}, \\ C_{\mathrm{ns}}^{+}(p_i^{e_i}), & \text{if } p_i \mid n_{\mathrm{ns}}^{+}. \end{cases} \tag{2.1}$$

Then we define our modular curves of mixed type as

$$X(n_0, n_{0^+}, n_{\mathrm{s}}, n_{\mathrm{s}^+}, n_{\mathrm{ns}}, n_{\mathrm{ns}^+}) := X_H / \langle w_{p_i}, \text{ for every prime } p_i \text{ dividing } n_{0^+} \rangle, \tag{2.2}$$

$$X(n_0, n_{0^+}, n_{\mathrm{ns}}, n_{\mathrm{ns}^+}) := X(n_0, n_{0^+}, 1, 1, n_{\mathrm{ns}}, n_{\mathrm{ns}^+}), \tag{2.3}$$

where w_{p_i} denotes the Atkin-Lehner operator associated to p_i. Let $n = p_1^{e_1} \cdots p_r^{e_r}$ be the prime factorization of n. We also define, for every positive integer n, the congruence subgroup

$$\Gamma_0(n) := \{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \quad \bmod n \},$$

we denote the $\mathbb{C}$-vector space of the cusp forms of weight 2 invariant under $\Gamma_0(n)$ by $\mathcal{S}_2(\Gamma_0(n))$ and by $\mathcal{S}_2^{\mathrm{new}}(\Gamma_0(n))$ the subspace generated by the newforms. We define the modular curve:

$$X_0(n) := \Gamma_0(n)\backslash\mathbb{H}^*.$$

We also denote the Jacobian of this curve by $J_0(n) := \mathrm{Jac}(X_0(n))$ and its new part by $J_0^{\mathrm{new}}(n)$, which is the factor of $J_0(n)$ isogenous to the abelian variety associated to $\mathcal{S}_2^{\mathrm{new}}(\Gamma_0(n))$.

Remark 2.4. There is an isomorphism of algebraic curves

$$X(n_0, n_{0^+}, n_{\mathrm{s}}, n_{\mathrm{s}^+}, n_{\mathrm{ns}}, n_{\mathrm{ns}^+}) \cong X(n_0 n_{\mathrm{s}}^2, n_{0^+} n_{\mathrm{s}^+}^2, n_{\mathrm{ns}}, n_{\mathrm{ns}^+}).$$

Indeed, writing the above curves respectively as $X_{H_1}/W_1 = \Gamma_1\backslash\mathbb{H}^*$ and $X_{H_2}/W_2 = \Gamma_2\backslash\mathbb{H}^*$, for Γ_1, Γ_2 subgroups of $\mathrm{PGL}_2^{\det>0}(\mathbb{R}) = \mathrm{Aut}(\mathbb{H})$, the group Γ_1 can be obtained conjugating Γ_2 firstly by $\left(\begin{smallmatrix} 0 & -1 \\ n_{\mathrm{s}} n_{\mathrm{s}^+} & 0 \end{smallmatrix}\right)$ and then conjugating again by a suitable matrix in $\mathrm{SL}_2(\mathbb{Z})$.

3. Jacobians of modular curves of mixed type and generalization of Chen's isogeny

With the notation introduced in Section 2, in this section we show that the Jacobian of the curves $X(n_0, n_{0^+}, n_{\mathrm{s}}, n_{\mathrm{s}^+}, n_{\mathrm{ns}}, n_{\mathrm{ns}^+})$ is isogenous to a product of Atkin-Lehner quotients of $J_0^{\mathrm{new}}(m)$ for suitable levels m. This generalizes a set of results beginning with Chen's work in [8] who proved the existence of an isogeny between the Jacobian of $X_{C_{\mathrm{ns}}(p)}$ and $J_0^{\mathrm{new}}(p^2)$, and between $X_{C_{\mathrm{ns}}^+(p)}$ and $J_0^{\mathrm{new}}(p^2)/\langle w_p\rangle$. This type of isogenies are often referred to as *Chen's isogenies*. We start with the key lemma where we discuss separately the four Cartan cases.

Lemma 3.1. *Let $n > 1$ be an integer and let $H < \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ be a subgroup. We use the following notation:*

$$J_0^{\mathrm{new}}(n)^{w_{p_1} w_{p_2} \dots w_{p_k}} := J_0^{\mathrm{new}}(n)/\langle w_{p_1}, w_{p_2}, \dots, w_{p_k}\rangle,$$

for $p_1, \dots, p_k$ distinct primes dividing n and w_{p_j} the Atkin-Lehner involution associated to p_j, for $j = 1, \dots, k$. Then we have:

(1) *If $H = C_{\mathrm{s}}(n) := \prod_{i=1}^r C_{\mathrm{s}}(p_i^{e_i})$, then*

$$\mathrm{Jac}(X_H) = J_{\mathrm{s}}(n) \sim \prod_{d \mid n^2} J_0^{\mathrm{new}}(d)^{\sigma_0\left(\frac{n^2}{d}\right)}, \tag{3.2}$$

where $\sigma_0(m)$ is the number of positive divisors of an integer m.

(2) *If* $H = C_{\mathrm{s}}^{+}(n) := \prod_{i=1}^{r} C_{\mathrm{s}}^{+}(p_i^{e_i})$, *then*

$$\mathrm{Jac}(X_H) = J_{\mathrm{s}}^{+}(n) \sim \prod_{d|n^2} J_0^{\mathrm{new}}(d)^{\sigma_0^*\left(\frac{n^2}{d}\right)}, \tag{3.3}$$

where σ_0^* *is the function defined by*

$$\sigma_0^*(p^f) := \begin{cases} \frac{1}{2}(f+1), & \textit{if } f \textit{ is odd}, \\ \frac{f}{2} + w_p, & \textit{if } f \textit{ is even}, \end{cases}$$

for a prime p *and a positive integer* f, *and* $\sigma_0^*(m_1 m_2) = \sigma_0^*(m_1)\sigma_0^*(m_2)$, *for* m_1, m_2 *coprime positive integers.*

(3) *If* $H = C_{\mathrm{ns}}(n) := \prod_{i=1}^{r} C_{\mathrm{ns}}(p_i^{e_i})$, *then*

$$\mathrm{Jac}(X_H) = J_{\mathrm{ns}}(n) \sim \prod_{d|n} J_0^{\mathrm{new}}(d^2). \tag{3.4}$$

(4) *If* $H = C_{\mathrm{ns}}^{+}(n) := \prod_{i=1}^{r} C_{\mathrm{ns}}^{+}(p_i^{e_i})$, *then*

$$\mathrm{Jac}(X_H) = J_{\mathrm{ns}}^{+}(n) \sim \prod_{d|n} J_0^{\mathrm{new}}(d^2)^{w_{p_1} \cdots w_{p_s}}, \tag{3.5}$$

where $p_1, \ldots, p_s$ *are all the primes dividing* d.

Proof. Part 1. We have

$$\mathrm{Jac}(X_H) = J_{\mathrm{s}}(n) \cong J_0(n^2),$$

because $W_n^{-1}\Gamma_{C_{\mathrm{s}}(n)}(n) W_n = \Gamma_0(n^2)$, where $W_n := \left(\begin{smallmatrix} 0 & -1 \\ n & 0 \end{smallmatrix}\right)$, and

$$J_0(n^2) \sim \prod_{d|n^2} J_0^{\mathrm{new}}(d)^{\sigma_0\left(\frac{n^2}{d}\right)},$$

because of classical Atkin-Lehner theory about the oldforms (see [14]).

Part 2. Let $n = p_1^{e_1} \ldots p_k^{e_k}$ be the prime factorization of n and let W_Q, for a positive integer Q, be the matrix defined in [2, after Lemma 7]. We have

$$\mathrm{Jac}(X_H) = J_{\mathrm{s}}^{+}(n) \cong J_0(n^2)^{w_{p_1} \cdots w_{p_k}},$$

because $\left(\begin{smallmatrix} 0 & -1 \\ n & 0 \end{smallmatrix}\right) \Gamma_{C_{\mathrm{s}}^{+}(n)} \left(\begin{smallmatrix} 0 & -1 \\ n & 0 \end{smallmatrix}\right)^{-1}$ is congruent to $\left\langle \Gamma_0(n^2), W_{p_1^{2e_1}}, \ldots, W_{p_k^{2e_k}} \right\rangle$ modulo scalar matrices. Then

$$J_0(n^2)^{w_{p_1} \cdots w_{p_k}} \sim \prod_{d|n^2} J_0^{\mathrm{new}}(d)^{\sigma_0^*\left(\frac{n^2}{d}\right)},$$

because of Atkin-Lehner theory (see [2, Equations 5.1 and 5.2]).

Part 3. Let $n = p_1^{e_1} \dots p_k^{e_k}$ be the prime factorization. For each $c = p_1^{f_1} \dots p_k^{f_k}$, we define

$$K(c) := \prod_{j=1}^{k} K_j(p_j^{f_j}) < \mathrm{GL}_2(\mathbb{Z}/c\mathbb{Z}), \quad \text{with} \quad K_j(p_j^{f_j}) := \begin{cases} T_{\frac{f_j}{2}}(p_j^{e_j}), & \text{if } f_j \text{ is even,} \\ B_{\frac{f_j-1}{2}}(p_j^{e_j}), & \text{if } f_j \text{ is odd.} \end{cases}$$

Then, using the machinery in [15] together with [11, Proposition 3.2], we get

$$\mathrm{Jac}(X_H) = J_{\mathrm{ns}}(n) \sim \prod_{c|n^2} \mathrm{Jac}(X_{K(c)})^{\varepsilon(c)m(c)},$$

where the functions $\varepsilon(c)$ and $m(c)$ are defined by

$$\varepsilon(p^f) := (-1)^f, \quad \text{and} \quad m(p^f) := \begin{cases} 1, & \text{if } p^f || n^2, \\ 2, & \text{otherwise,} \end{cases} \tag{3.6}$$

for a prime power dividing n^2 and by $\varepsilon(d_1 d_2) = \varepsilon(d_1)\varepsilon(d_2)$ and $m(d_1 d_2) = m(d_1)m(d_2)$ for d_1, d_2 coprime divisors of n^2. (For example if $n^2 = p^2 q^2$ and $c = p = p^1 q^0$, then $m(c) = m(p^1)m(q^0) = 4$.) Moreover, we have

$$\prod_{c|n^2} \mathrm{Jac}(X_{K(c)})^{\varepsilon(c)m(c)} \cong \prod_{c|n^2} J_0(c)^{\varepsilon(c)m(c)},$$

because $\Gamma_{K(c)}$ and $\Gamma_0(c)$ are conjugate, as explained in [11, proof of Theorem 3.8]. Then we have

$$\prod_{c|n^2} J_0(c)^{\varepsilon(c)m(c)} \sim \prod_{c|n^2} \prod_{d|c} J_0^{\mathrm{new}}(d)^{\varepsilon(c)m(c)\sigma_0(\frac{c}{d})},$$

because of classical Atkin-Lehner theory about the oldforms (see [14]). Last equality:

$$\prod_{c|n^2} \prod_{d|c} J_0^{\mathrm{new}}(d)^{\varepsilon(c)m(c)\sigma_0(\frac{c}{d})} = \prod_{d|n} J_0^{\mathrm{new}}(d^2),$$

follows by

$$\begin{aligned} \prod_{c|n^2} \prod_{d|c} J_0^{\mathrm{new}}(d)^{\varepsilon(c)m(c)\sigma_0(\frac{c}{d})} &= \prod_{d|n^2} \prod_{d|c|n^2} J_0^{\mathrm{new}}(d)^{\varepsilon(c)m(c)\sigma_0(\frac{c}{d})} = \\ &= \prod_{d|n^2} J_0^{\mathrm{new}}(d)^{\sum_{d|c|n^2} \varepsilon(c)m(c)\sigma_0(\frac{c}{d})}; \end{aligned}$$

and, if $n = p_1^{e_1} \dots p_k^{e_k}$ and $d = p_1^{g_1} \dots p_k^{g_k}$ and $c = p_1^{f_1} \dots p_k^{f_k}$ are the prime factorizations of n, d, c, we have

$$\sum_{d|c|n^2} \varepsilon(c)m(c)\sigma_0\left(\frac{c}{d}\right) = \sum_{f_1=g_1}^{2e_1} \cdots \sum_{f_k=g_k}^{2e_k} \varepsilon(p_1^{f_1}\dots p_k^{f_k})m(p_1^{f_1}\dots p_k^{f_k})\sigma_0\left(p_1^{f_1-g_1}\dots p_k^{f_k-g_k}\right) =$$
$$= \prod_{j=1}^{k}\sum_{f_j=g_j}^{2e_j} \varepsilon(p_j^{f_j})m(p_j^{f_j})\sigma_0\left(p_j^{f_j-g_j}\right) = \prod_{j=1}^{k}\left(2e_j - g_j + 1 + \sum_{f_j=g_j}^{2e_j-1}(-1)^{f_j}2(f_j-g_j+1)\right) =$$
$$= \prod_{j=1}^{k}\left(2e_j - g_j + 1 + 2\sum_{f_j=g_j}^{2e_j-1}(-1)^{f_j}f_j + 2(1-g_j)\sum_{f_j=g_j}^{2e_j-1}(-1)^{f_j}\right) = \prod_{j=1}^{k}\left(\frac{1}{2}(1+(-1)^{g_j})\right) =$$
$$= \begin{cases} 1, & \text{if } g_1 \equiv \ldots \equiv g_k \equiv 0 \bmod 2, \\ 0, & \text{otherwise,} \end{cases}$$

where in the fifth equality we used

$$\sum_{i=a}^{b-1} x^i = \frac{x^a - x^b}{1-x} \quad \text{and} \quad \sum_{i=a}^{b-1} i x^{i-1} = \frac{x^a - x^b}{(1-x)^2} + \frac{ax^{a-1} - bx^{b-1}}{1-x},$$

hence

$$\prod_{d|n^2} J_0^{\text{new}}(d)^{\sum_{d|c|n^2}\varepsilon(c)m(c)\sigma_0\left(\frac{c}{d}\right)} = \prod_{d|n} J_0^{\text{new}}(d^2).$$

Part 4. Given the factorization $n = p_1^{e_1}\dots p_k^{e_k}$, for each $c = p_1^{f_1}\dots p_k^{f_k}$, we define

$$K'(c) := \prod_{j=1}^{k} K'_j(p_j^{f_j}) < \mathrm{GL}_2(\mathbb{Z}/c\mathbb{Z}), \text{ with } K'_j(p_j^{f_j}) := \begin{cases} T_{\frac{f_j}{2}}(p_j^{e_j}), & \text{if } f_j \neq 2e_j \text{ and even,} \\ C_{\mathrm{s}}^{+}(p_j^{e_j}), & \text{if } f_j = 2e_j, \\ B_{\frac{f_j-1}{2}}(p_j^{e_j}), & \text{if } f_j \text{ is odd.} \end{cases}$$

Then, using the machinery explained in [15], together with [9, Theorem 1.1] and its extension to the even case described in Section 3 and in the appendix of [11], we get

$$\mathrm{Jac}(X_H) = J_{\mathrm{ns}}^{+}(n) \sim \prod_{c|n^2} \mathrm{Jac}(X_{K'(c)})^{\varepsilon(c)},$$

where ε is defined as in the proof of Part 3.

Then, defining the matrices W_Q, for a positive integer Q, as in [2, after Lemma 7] and since $\left(\begin{smallmatrix} 0 & -1 \\ m & 0 \end{smallmatrix}\right)\Gamma_{K'(c)}\left(\begin{smallmatrix} 0 & -1 \\ m & 0 \end{smallmatrix}\right)^{-1}$ is congruent to $\left\langle \Gamma_0(c), W_{p_j^{f_j}} \text{ for } p_j|c \text{ s.t. } f_j = 2e_j \right\rangle$ modulo scalar matrices, where m is such that $c = m^2 \prod_{\substack{j=1 \\ f_j \text{ odd}}}^{k} p_j$, we have

$$\prod_{c|n^2} \mathrm{Jac}(X_{K'(c)})^{\varepsilon(c)} \cong \prod_{c|n^2} J_0(c)^{\varepsilon(c)\prod' w_{p_j}},$$

where

$$\prod{}' w_{p_j} := \prod_{\substack{p_j | c \text{ s.t.} \\ f_j = 2e_j}} w_{p_j}.$$

Then

$$\prod_{c|n^2} J_0(c)^{\varepsilon(c)\prod' w_{p_j}} \sim \prod_{c|n^2}\prod_{d|c} J_0^{\mathrm{new}}(d)^{\varepsilon(c)\sigma_0'(\frac{c}{d})},$$

is similar to Parts 1 and 2, where

$$\sigma_0'(p^f) := \begin{cases} \sigma_0^*(p^f), & \text{if } p^f || \frac{n^2}{d}, \\ \sigma_0(p^f), & \text{otherwise,} \end{cases} \tag{3.7}$$

for a prime power dividing $\frac{n^2}{d}$ and $\sigma_0'(d_1 d_2) = \sigma_0'(d_1)\sigma_0'(d_2)$ for d_1, d_2 coprime divisors of $\frac{n^2}{d}$. Last equality:

$$\prod_{c|n^2}\prod_{d|c} J_0^{\mathrm{new}}(d)^{\varepsilon(c)\sigma_0'(\frac{c}{d})} = \prod_{d|n} J_0^{\mathrm{new}}(d^2)^{w_{p_1}\dots w_{p_k}},$$

follows by

$$\begin{aligned}\prod_{c|n^2}\prod_{d|c} J_0^{\mathrm{new}}(d)^{\varepsilon(c)\sigma_0'(\frac{c}{d})} &= \prod_{d|n^2}\prod_{d|c|n^2} J_0^{\mathrm{new}}(d)^{\varepsilon(c)\sigma_0'(\frac{c}{d})} = \\ &= \prod_{d|n^2} J_0^{\mathrm{new}}(d)^{\sum_{d|c|n^2}\varepsilon(c)\sigma_0'(\frac{c}{d})};\end{aligned}$$

and, if $d = p_1^{g_1}\dots p_k^{g_k}$ is the prime factorization of d, we have

$$\begin{aligned}&\sum_{d|c|n^2}\varepsilon(c)\sigma_0'\left(\frac{c}{d}\right) = \sum_{f_1=g_1}^{2e_1}\dots\sum_{f_k=g_k}^{2e_k}\varepsilon(p_1^{f_1}\dots p_k^{f_k})\sigma_0'\left(p_1^{f_1-g_1}\dots p_k^{f_k-g_k}\right) = \\ &= \prod_{j=1}^{k}\sum_{f_j=g_j}^{2e_j}\varepsilon(p_j^{f_j})\sigma_0'\left(p_j^{f_j-g_j}\right) = \prod_{j=1}^{k}\left(\sigma_0^*\left(p_j^{2e_j-g_j}\right) + \sum_{f_j=g_j}^{2e_j-1}(-1)^{f_j}(f_j-g_j+1)\right) = \\ &= \prod_{j=1}^{k}\left(\sigma_0^*\left(p_j^{2e_j-g_j}\right) + \sum_{f_j=g_j}^{2e_j-1}(-1)^{f_j}f_j + (1-g_j)\sum_{f_j=g_j}^{2e_j-1}(-1)^{f_j}\right) = \\ &= \prod_{j=1}^{k}\left(\sigma_0^*\left(p_j^{2e_j-g_j}\right) - e + \frac{1}{4}\Big((-1)^{g_j} - 1 + 2g_j\Big)\right) =\end{aligned}$$

$$= \begin{cases} \prod_{j=1}^{k} w_{p_j}, & \text{if } g_1 \equiv \ldots \equiv g_k \equiv 0 \bmod 2, \\ 0, & \text{otherwise,} \end{cases}$$

where in the fifth equality we used

$$\sum_{i=a}^{b-1} x^i = \frac{x^a - x^b}{1-x} \quad \text{and} \quad \sum_{i=a}^{b-1} i x^{i-1} = \frac{x^a - x^b}{(1-x)^2} + \frac{a x^{a-1} - b x^{b-1}}{1-x},$$

hence

$$\prod_{d \mid n^2} J_0^{\text{new}}(d)^{\sum_{d|c|n^2} \varepsilon(c) \sigma_0'(\frac{c}{d})} = \prod_{d \mid n} J_0^{\text{new}}(d^2)^{w_{p_1} \ldots w_{p_k}}. \quad \square$$

Theorem 3.8. *Let $X := X(n_0, n_{0+}, n_{\mathrm{s}}, n_{\mathrm{s}+}, n_{\mathrm{ns}}, n_{\mathrm{ns}+})$ be as in Equation (2.2), then*

$$\operatorname{Jac}(X) \sim \prod_{d \mid N} J_0^{\text{new}}(d_0 d_{0+} d_{\mathrm{s}} d_{\mathrm{s}+} d_{\mathrm{ns}}^2 d_{\mathrm{ns}+}^2)^{\sigma_0\left(\frac{n_0 n_{\mathrm{s}}^2}{d_0 d_{\mathrm{s}}}\right) \sigma_0^*\left(\frac{n_{0+} n_{\mathrm{s}+}^2}{d_{0+} d_{\mathrm{s}+}}\right) \prod_{p \in \mathcal{P}(d_{\mathrm{ns}+})} w_p}, \tag{3.9}$$

where $N := n_0 n_{0+} n_{\mathrm{s}}^2 n_{\mathrm{s}+}^2 n_{\mathrm{ns}} n_{\mathrm{ns}+}$ and $d := d_0 d_{0+} d_{\mathrm{s}} d_{\mathrm{s}+} d_{\mathrm{ns}} d_{\mathrm{ns}+}$, with $d_0 \mid n_0$, $d_{0+} | n_{0+}$, $d_{\mathrm{s}} | n_{\mathrm{s}}^2$, $d_{\mathrm{s}+} | n_{\mathrm{s}+}^2$, $d_{\mathrm{ns}} | n_{\mathrm{ns}}$, $d_{\mathrm{ns}+} | n_{\mathrm{ns}+}$, and

$$J_0^{\text{new}}(p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k})^{w_{p_1} w_{p_2} \ldots w_{p_k}} := J_0^{\text{new}}(p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}) / \langle w_{p_1}, w_{p_2}, \ldots, w_{p_k} \rangle,$$

for $p_1, \ldots, p_k$ distinct primes and w_{p_j} is the Atkin-Lehner involution associated to p_j, for $j = 1, \ldots, k$; moreover $\mathcal{P}(m)$ is the set of prime divisors of an integer m and $\sigma_0(m)$ is the number of positive divisors of m and σ_0^* is the function defined by

$$\sigma_0^*(p^f) := \begin{cases} \frac{1}{2}(f+1), & \text{if } f \text{ is odd,} \\ \frac{f}{2} + w_p, & \text{if } f \text{ is even,} \end{cases}$$

for a prime p and a positive integer f, and $\sigma_0^*(m_1 m_2) = \sigma_0^*(m_1) \sigma_0^*(m_2)$, for m_1, m_2 coprime positive integers.

Proof. This is a natural extension of the previous lemma and the argument is the same. Given c_{ns} and $c_{\mathrm{ns}+}$ divisors of n_{ns}^2 and $n_{\mathrm{ns}+}^2$ respectively, for each $c := n_0 n_{0+} n_{\mathrm{s}} n_{\mathrm{s}+} c_{\mathrm{ns}} c_{\mathrm{ns}+}$, we define

$$K(c) := \prod_{\substack{p^f \| c \\ p \text{ prime}}} K(p^f),$$

where, if e is the p-adic valuation of n, we define

$$K(p^f) := \begin{cases} B^0(p^f), & \text{if } p|n_0 n_{0^+}, \\ C_{\mathrm{s}}(p^f), & \text{if } p|n_{\mathrm{s}}, \\ C_{\mathrm{s}}^+(p^f), & \text{if } p|n_{\mathrm{s}^+}, \\ B_{\frac{f-1}{2}}(p^e), & \text{if } p|c_{\mathrm{ns}}c_{\mathrm{ns}^+} \text{ and if } f \text{ is odd}, \\ T_{\frac{f}{2}}(p^e), & \text{if } p|c_{\mathrm{ns}}c_{\mathrm{ns}^+} \text{ and } f \text{ is even and } f \neq 2e, \\ C_{\mathrm{s}}(p^e), & \text{if } p|c_{\mathrm{ns}} \text{ and } f = 2e, \\ C_{\mathrm{s}}^+(p^e), & \text{if } p|c_{\mathrm{ns}^+} \text{ and } f = 2e. \end{cases}$$

Again, using the machinery explained in [15], together with the representation theoretic results in [9] and [11], and defining ε, m, σ_0' as in Equations (3.6) and (3.7), we find that

$$\begin{aligned}
&\mathrm{Jac}(X_H)^{\prod w_{p_{0^+}}} \sim \\
&\sim \prod_{\substack{c_{\mathrm{ns}}|n_{\mathrm{ns}}^2 \\ c_{\mathrm{ns}^+}|n_{\mathrm{ns}^+}^2}} \mathrm{Jac}(X_{K(n_0 n_{0^+} n_{\mathrm{s}} n_{\mathrm{s}^+} c_{\mathrm{ns}} c_{\mathrm{ns}^+})})^{\varepsilon(c_{\mathrm{ns}})\varepsilon(c_{\mathrm{ns}^+})m(c_{\mathrm{ns}})\prod w_{p_{0^+}}} \cong \\
&\cong \prod_{\substack{c_{\mathrm{ns}}|n_{\mathrm{ns}}^2 \\ c_{\mathrm{ns}^+}|n_{\mathrm{ns}^+}^2}} J_0(n_0 n_{0^+} n_{\mathrm{s}}^2 n_{\mathrm{s}^+}^2 c_{\mathrm{ns}} c_{\mathrm{ns}^+})^{\varepsilon(c_{\mathrm{ns}})\varepsilon(c_{\mathrm{ns}^+})m(c_{\mathrm{ns}})\prod w_{p_{0^+}} \prod w_{p_{\mathrm{s}^+}} \prod' w_{p_{\mathrm{ns}^+}}} \sim \\
&\sim \prod_{\substack{c_{\mathrm{ns}}|n_{\mathrm{ns}}^2 \\ c_{\mathrm{ns}^+}|n_{\mathrm{ns}^+}^2}} \prod_{d|N} J_0^{\mathrm{new}}(d)^{\varepsilon(c_{\mathrm{ns}})\varepsilon(c_{\mathrm{ns}^+})m(c_{\mathrm{ns}})\sigma_0\left(\frac{n_0}{d_0}\right)\sigma_0^*\left(\frac{n_{0^+}}{d_{0^+}}\right)\sigma_0\left(\frac{n_{\mathrm{s}}^2}{d_{\mathrm{s}}}\right)\sigma_0^*\left(\frac{n_{\mathrm{s}^+}^2}{d_{\mathrm{s}^+}}\right)\sigma_0\left(\frac{c_{\mathrm{ns}}}{d_{\mathrm{ns}}}\right)\sigma_0'\left(\frac{c_{\mathrm{ns}^+}}{d_{\mathrm{ns}^+}}\right)} = \\
&= \prod_{d|N} J_0^{\mathrm{new}}(d_0 d_{0^+} d_{\mathrm{s}} d_{\mathrm{s}^+} d_{\mathrm{ns}}^2 d_{\mathrm{ns}^+}^2)^{\sigma_0\left(\frac{n_0}{d_0}\right)\sigma_0^*\left(\frac{n_{0^+}}{d_{0^+}}\right)\sigma_0\left(\frac{n_{\mathrm{s}}^2}{d_{\mathrm{s}}}\right)\sigma_0^*\left(\frac{n_{\mathrm{s}^+}^2}{d_{\mathrm{s}^+}}\right)\prod w_{p_{\mathrm{ns}^+}}},
\end{aligned}$$

where d and N are defined in the statement of the theorem and the product $\prod w_{p_{0^+}}$ varies over all the primes p_{0^+} dividing n_{0^+}, the product $\prod w_{p_{\mathrm{s}^+}}$ varies over all the primes p_{s^+} dividing c_{s^+}, the product $\prod w_{p_{\mathrm{ns}^+}}$ varies over all the primes p_{ns^+} dividing n_{ns^+} and the product $\prod' w_{p_{\mathrm{ns}^+}}$ varies over all the primes p_{ns^+} such that $v_{p_{\mathrm{ns}^+}}(c_{\mathrm{ns}^+}) = v_{p_{\mathrm{ns}^+}}(n_{\mathrm{ns}^+}^2)$, where $v_p(m)$ is the exponent of the prime p in the prime factorization of m. $\square$

4. Computing the number of points

Let p and ℓ be distinct primes. Let C be a smooth, projective, algebraic curve over $\mathbb{Q}$ with good reduction over $\mathbb{F}_p$. Let $\mathrm{Ta}_\ell(\mathrm{Jac}(C))$ be the Tate module of C, i.e., the inverse limit of the ℓ^m-torsion group $\mathrm{Jac}(C)[\ell^m]$, and let $V_\ell = \mathrm{Ta}_\ell(\mathrm{Jac}(C)) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ be the $\mathbb{Q}_\ell$-vector space associated to $\mathrm{Ta}_\ell(\mathrm{Jac}(C))$. The trace of the Frobenius automorphism Frob_{p^k} acting on V_ℓ satisfies:

$$\mathrm{tr}(\mathrm{Frob}_{p^k}|V_\ell) = p^k + 1 - \#C(\mathbb{F}_{p^k}), \tag{4.1}$$

for every positive integer k. (see [21, Theorem 11.1]). When C is a modular curve associated to a group of matrices containing the scalar matrices, the Eichler-Shimura relation (see [14, Theorem 8.7.2]) implies that the trace of Frobenius can be obtained from a linear combination of traces of Hecke operators, as we explain in Section 5.

We are interested in applying Equation (4.1) when $C = X(n_0, n_{0+}, n_{\mathrm{s}}, n_{\mathrm{s}+}, n_{\mathrm{ns}}, n_{\mathrm{ns}+})$ as in Equation (2.2) and p does not divide $n = n_0\, n_{0+} n_{\mathrm{s}} n_{\mathrm{s}+} n_{\mathrm{ns}} n_{\mathrm{ns}+}$. Using Theorem 3.8, the number of points over $\mathbb{F}_p$ can be computed in terms of the eigenvalues of the Hecke operator $T_p \in \mathrm{End}(J_0^{\mathrm{new}}(d))$, whose level d divides n. By [14, Theorem 6.6.6], we have that $J_0^{\mathrm{new}}(d)$ is isogenous to a direct sum $\bigoplus_f A_f^{\sigma_0(d/d')}$ of Abelian varieties A_f associated to the Galois orbits of the normalized eigenforms $f \in \mathcal{S}_2(\Gamma_0(d'))$, where $d' \mid d$. In the following part of this section we explain how to compute $\mathrm{tr}(\mathrm{Frob}_p|V_\ell)$ explicitly when $C = X_H$. This, by Equation (4.1) above, allows to compute the number of points of X_H on $\mathbb{F}_p$. Finally, we explain how to compute the number of points of X_H on every finite field (not only prime fields). The following lemma is well known, but we report the proof for convenience of the reader.

Lemma 4.2. *Let n be a positive integer, let p, ℓ be distinct primes not dividing n and let $V_\ell = \mathrm{Ta}_\ell(J_0(n)_{\mathbb{F}_p}) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ be the $\mathbb{Q}_\ell$-vector space associated to the Tate module of $X_0(n)_{\mathbb{F}_p}$. Then*

$$\mathrm{tr}_{\mathbb{T}}(\mathrm{Frob}_p|V_\ell) = T_p,$$

where T_p is the Hecke operator associated to the prime p and the trace is taken on V_ℓ as $\mathbb{T}_{\mathbb{Q}_\ell}$-module with $\mathbb{T}_{\mathbb{Q}_\ell} := \mathbb{T}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$ and $\mathbb{T}_{\mathbb{Z}}$ denotes the Hecke algebra $\mathbb{Z}[T_n : n > 0]$.

Proof. We have that V_ℓ is a free rank 2 module over $\mathbb{T}_{\mathbb{Q}_\ell}$ (see [14, Lemma 9.5.3]). Consider the Weil pairing $\langle\cdot,\cdot\rangle\colon V_\ell \times V_\ell \to \mathbb{Q}_\ell(1)$, see [20, before Lemma 16.2, p. 132] where we identify $J_0(n)$ with its dual variety via the principal polarization. Let V_ℓ^* be the dual module of V_ℓ where for every linear operator $T\colon V_\ell \to V_\ell$ we have the dual action on V_ℓ^*, i.e., $T\varphi := \varphi \circ T$, for every $\varphi \in V_\ell^*$. Let $\Phi\colon V_\ell \to V_\ell^*$ be the isomorphism sending x in the map $\Phi_x\colon V_\ell \to \mathbb{Q}_\ell$ defined by $\Phi_x(y) := \langle y, x\rangle$. Each Hecke operator T_n is self-adjoint with respect to the Weil pairing, see Lemma 4.3 below. This implies that Φ commutes with the natural action of $\mathbb{T}_{\mathbb{Q}_\ell}$ on each side, i.e., Φ is a isomorphism of $\mathbb{T}_{\mathbb{Q}_\ell}$-modules.

The Verschiebung $\mathrm{Ver}_p = [p]\mathrm{Frob}_p^{-1}$ is the dual isogeny of Frob_p on Jacobians and it is the adjoint of Frob_p with respect to Weil pairing, in fact: $\langle x, \mathrm{Ver}_p(y)\rangle = \langle x, [p]\mathrm{Frob}_p^{-1}(y)\rangle = \langle x, \mathrm{Frob}_p^{-1}(y)\rangle^p = \mathrm{Frob}_p(\langle x, \mathrm{Frob}_p^{-1}(y)\rangle) = \langle \mathrm{Frob}_p(x), \mathrm{Frob}_p(\mathrm{Frob}_p^{-1}(y))\rangle = \langle \mathrm{Frob}_p(x), y\rangle$. Hence $\Phi \circ \mathrm{Frob}_p = \mathrm{Ver}_p \circ \Phi$. This implies that $\mathrm{tr}_{\mathbb{T}}(\mathrm{Frob}_p|V_\ell) = \mathrm{tr}_{\mathbb{T}}(\mathrm{Ver}_p|V_\ell^*)$. But, with respect to a fixed basis on V_ℓ and its dual basis on V_ℓ^*, the matrix of Ver_p on V_ℓ^* is the transpose of the matrix of Ver_p on V_ℓ, so $\mathrm{tr}_{\mathbb{T}}(\mathrm{Frob}_p|V_\ell) = \mathrm{tr}_{\mathbb{T}}(\mathrm{Ver}_p|V_\ell)$. Applying the trace to the Eichler-Shimura relation $\mathrm{Frob}_p + \mathrm{Ver}_p = T_p$ (see [14, Theorem 8.7.2]), we get $2\mathrm{tr}_{\mathbb{T}}(\mathrm{Frob}_p|V_\ell) = \mathrm{tr}_{\mathbb{T}}(T_p|V_\ell) = 2T_p$ and, hence $\mathrm{tr}_{\mathbb{T}}(\mathrm{Frob}_p|V_\ell) = T_p$. □

Lemma 4.3. *For all pairwise coprime positive integers N, n, ℓ, with ℓ prime, the Hecke operator T_n is self-adjoint with respect to the Weil pairing on $J_0(N)[\ell^m]$.*

Proof. Since T_n can be written as a polynomial in the operators T_p for primes p dividing n and all these T_p's commute with each other, then it is enough to treat the case where $n = p$ is prime.

We focus on the action of T_p on divisors supported on non-cuspidal points. Indeed, since the number of cusps is finite, each element of $J_0(N)$ can be represented as a divisor supported in the non-cuspidal locus. We recall that the non-cuspidal points of $X_0(N)$ parametrize data (E, G), where E is an elliptic curve and G is a cyclic subgroup of order N of $E[N]$ and the non-cuspidal points of $X_0(Np)$ parametrize data $(E, \varphi\colon E \to E', G)$, for E, G as before and φ an isogeny of degree p. With this notation, let $p_1, p_2\colon X_0(Np) \to X_0(N)$ be the maps defined by

$$p_1(E, \varphi\colon E \to E', G) = (E, G), \quad p_2(E, \varphi\colon E \to E', G) = (E', \varphi(G)),$$

and extended by continuity on the whole curve. Then $T_p = (p_2)_* p_1^*$ as an endomorphism of the Jacobian.

We recall that for each non-constant map of curves $f\colon C \to C'$, the maps f^* and f_* between the two Jacobians are adjoint with respect to the Weil pairings. Indeed, given divisors D, D' respectively on C, C' that define N-torsion points in the respective Jacobians and such that $f_*(D)$ is disjoint from D', take rational functions g, g' such with $\operatorname{div}(g) = ND$ and $\operatorname{div}(g') = ND'$, so that

$$\langle D, f^* D' \rangle = \frac{g(f^* D')}{(g' \circ f)(D)} = \frac{(\operatorname{Norm}_f g)(D')}{(g'(f_*(D))} = \langle f_* D, D' \rangle,$$

where $\langle , \rangle$ denotes the Weil pairing on the N-torsion subgroup and Norm_f is the norm of the finite extension of function fields $f^{\#}\colon K(C') \hookrightarrow K(C)$, namely for each rational function h on C' we denote $\operatorname{Norm}_f(h) = \det_{K(C)}(\cdot h\colon K(C') \to K(C')) \in K(C)$.

As a consequence of the above general fact, the adjoint of T_p is $T_p^* = (p_1)_* p_2^*$, i.e., it is induced by the transposed correspondence of T_p. Hence, to prove our statement, it is enough proving that the image of the map $(p_1, p_2)\colon X_0(Np) \to X_0(N) \times X_0(N)$ is symmetric. Indeed, given $x = (E, G)$, $y = (E', G')$ in $X_0(N) \times X_0(N)$, the point (x, y) lies in the image of (p_1, p_2) if and only if there exists an isogeny $\varphi\colon E \to E'$ of degree p such that $\varphi(G) = G'$. If this happens, then the dual isogeny $\hat{\varphi}\colon E' \to E$ sends G' into G, since $G = [p]G = \hat{\varphi}(\varphi(G)) = \hat{\varphi}(G')$. In other words whenever (x, y) lies in the image of (p_1, p_2), then (y, x) lies in the same image, i.e., the image of (p_1, p_2) is symmetric. □

The following proposition explains how to compute $\operatorname{tr}(\operatorname{Frob}_p | V_\ell)$ explicitly when the abelian variety considered is not necessarily a Jacobian but it is a product of A_f for $f \in \mathcal{S}_2^{\text{new}}(\Gamma_0(n_f))$, where $n_f \in \mathbb{Z}_{>0}$ is the level of f. It implies the case we are interested in: $C = X_H$ for H as described in the statement of Theorem 3.8.

Proposition 4.4. *Let $\mathcal{F}$ be a finite subset of the set of the Galois orbits of normalized eigenforms of $\bigcup_{n>0} \mathcal{S}_2^{\mathrm{new}}(\Gamma_0(n))$, and let $J := \prod_{[f]\in\mathcal{F}} A_f^{m_f}$, where A_f is the abelian variety associated to Galois orbit of f (see [14, Definition 6.6.3]) and $m_f \in \mathbb{Z}_{>0}$. Moreover, let $V_\ell = \mathrm{Ta}_\ell(J) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ be the $\mathbb{Q}_\ell$-vector space associated to the Tate module of J. Then the characteristic polynomial of Frob_p acting on V_ℓ is*

$$\prod_{[f]\in\mathcal{F}} \prod_{h\in[f]} (x^2 - a_p(h)x + p)^{m_f},$$

where $a_p(h)$ is the p-th Fourier coefficient of h.

Proof. It is enough to treat the case $\mathcal{F} = \{[f]\}$ for f an eigenform of level n. Let

$$S := \bigoplus_{h\in[f]} \mathbb{C}h \quad \subset \mathcal{S}_2^{\mathrm{new}}(\Gamma_0(n)),$$

and let $\mathbb{T}$ be the Hecke algebra of A_f defined as the maximal quotient of the Hecke algebra $\mathbb{T}'$ of $J_0(n)$ such that the action of $\mathbb{T}'$ on A_f acts through $\mathbb{T}$. Also, for each ring R, let $\mathbb{T}_R := \mathbb{T} \otimes R$.

By [14, Lemma 9.5.3], V_ℓ is a free module of rank 2 over $\mathbb{T}_{\mathbb{Q}_\ell}$, and the characteristic polynomial of Frob_p as a $\mathbb{T}_{\mathbb{Q}_\ell}$-linear endomorphism is x^2-T_px+p. Indeed, by Lemma 4.2 this characteristic polynomial is of the form $x^2 - T_px + a$ for a certain $a \in \mathbb{T}_{\mathbb{Q}_\ell}$. Since $\mathbb{T}_{\mathbb{Q}_\ell}$ acts faithfully on V_ℓ, the element a is the unique element of $\mathbb{T}_{\mathbb{Q}_\ell}$ such that $\mathrm{Frob}_p^2 - T_p\mathrm{Frob}_p + a = 0$, and $a = p$ satisfies this property because, by Eichler-Shimura Relation and denoting by Ver_p the Verschiebung operator, we have

$$\begin{aligned}\mathrm{Frob}_p^2 - T_p\mathrm{Frob}_p + p = \mathrm{Frob}_p^2 - (\mathrm{Frob}_p + \mathrm{Ver}_p)\mathrm{Frob}_p + \mathrm{Frob}_p\mathrm{Ver}_p =\\ = (\mathrm{Frob}_p - \mathrm{Ver}_p)(\mathrm{Frob}_p - \mathrm{Frob}_p) = 0.\end{aligned}$$

In particular, the characteristic polynomial of Frob_p as a $\mathbb{Q}_\ell$-linear endomorphism of V_ℓ is

$$\begin{aligned}&\det{}_{\mathbb{Q}_\ell[x]}(\mathrm{Frob}_p - x|V_\ell \otimes_{\mathbb{Q}_\ell} \mathbb{Q}_\ell[x])\\ &\quad= \mathrm{Norm}_{\mathbb{T}_{\mathbb{Q}_\ell}[x]/\mathbb{Q}_\ell[x]}\Big(\det{}_{\mathbb{T}_{\mathbb{Q}_\ell}[x]}(\mathrm{Frob}_p - x|V_\ell \otimes_{\mathbb{Q}_\ell} \mathbb{Q}_\ell[x])\Big) =\\ &\quad= \mathrm{Norm}_{\mathbb{T}_{\mathbb{Q}_\ell}[x]/\mathbb{Q}_\ell[x]}(x^2 - T_px + p) = \mathrm{Norm}_{\mathbb{T}_{\mathbb{Q}}[x]/\mathbb{Q}[x]}(x^2 - T_px + p) =\\ &\quad= \mathrm{Norm}_{\mathbb{T}_{\mathbb{C}}[x]/\mathbb{C}[x]}(x^2 - T_px + p),\end{aligned}$$

where, given a ring extension $A \subset B$ such that B is a finite, free A-module, we denote $\mathrm{Norm}_{B/A}(t) := \det_A(\cdot t\colon B \to B)$, i.e., the determinant of the multiplication by t inside B as a A-module endomorphism. Since S is a free $\mathbb{T}_{\mathbb{C}}$-module of rank 1, then $S \cong \mathbb{T}_{\mathbb{C}}$ as $\mathbb{T}_{\mathbb{C}}$-modules, hence,

$$\mathrm{Norm}_{\mathbb{T}_{\mathbb{C}}[x]/\mathbb{C}[x]}(x^2 - T_p x + p) = \det{}_{\mathbb{C}[x]}(x^2 - T_p x + p | S \otimes_{\mathbb{C}} \mathbb{C}[x]) = \prod_{h \in [f]} (x^2 - a_p(h)x + p),$$

where the last equality is true because the elements $h \in [f]$ are a basis of eigenvectors for T_p in S, with eigenvalue $a_p(h)$. □

Using Theorem 3.8 and Formula 4.2 above we can compute $\#X(n_0, n_{0^+}, n_{\mathrm{ns}}, n_{\mathrm{ns}^+})(\mathbb{F}_q)$ for all prime power $q = p^k$ not dividing $n = n_0 n_{0^+} n_{\mathrm{ns}} n_{\mathrm{ns}^+}$. We concentrate on these cases because of the isomorphism of Remark 2.4. The algorithm runs as follows:

Algorithm 4.5. *Computing the number of points of $X(n_0, n_{0^+}, n_{\mathrm{ns}}, n_{\mathrm{ns}^+})$ over $\mathbb{F}_q$.*

(1) For every $d|n$, compute $d_0 := \gcd(n_0, d)$ and similarly d_0^+, d_{ns} and d_{ns^+} and let $D := d_0 d_0^+ d_{\mathrm{ns}}^2 d_{\mathrm{ns}^+}^2$.
(2) For every $d|n$, choose a basis $\mathcal{B}(d)$ of new eigenforms of level D and let $\mathcal{B} := \bigcup_{d|n} \mathcal{B}(d)$ be the union of these bases.
(3) For every $d \mid n$ and for each prime $\ell \mid d_{\mathrm{ns}}^+$, compute the eigenvalue of $f \in \mathcal{B}(d)$ with respect to the Atkin-Lehner operator w_ℓ and discard from $\mathcal{B}$ the f's with eigenvalue -1 (these data are available on the database [18] for $D \leqslant 10000$).
(4) Compute the Hecke eigenvalue $a_p(f)$ for every $f \in \mathcal{B}$ (these data are available on the database [18] for $D \leqslant 10000$).
(5) For each $f \in \mathcal{B}$, compute $m_f := \sigma_0(n_0/d_0)\tilde{\sigma}_0(n_{0^+}/d_{0^+}, f)$, where $\sigma_0(m)$ is the number of positive divisors of m and $m \mapsto \tilde{\sigma}_0(m, f)$ is the multiplicative function defined by

$$\tilde{\sigma}_0(p^r, f) := \begin{cases} \frac{1}{2}(r+1), & \text{if } r \text{ is odd}, \\ \frac{r}{2}+1, & \text{if } r \text{ is even and } w_p f = f, \\ \frac{r}{2}, & \text{if } r \text{ is even and } w_p f = -f. \end{cases}$$

(6) If $k = 1$, then compute Frobenius traces acting on A_f: $\mathrm{tr}(\mathrm{Frob}_p | A_f) = \sum_{h \in [f]} a_p(h)$, where $[f]$ is the Galois orbit of f.
(7) If $k > 1$, then compute the (complex) roots $\alpha(h)$ and $\beta(h)$ of quadratic the polynomial $x^2 - a_p(h)x + p = 0$, for each $h \in [f]$. Then compute $\mathrm{tr}(\mathrm{Frob}_q | A_f) = \sum_{h \in [f]} (\alpha(h)^k + \beta(h)^k)$, using Equation (4.1)
(8) Finally, $\#X(n_0, n_{0^+}, n_{\mathrm{ns}}, n_{\mathrm{ns}^+})(\mathbb{F}_q) = q + 1 - \sum_{[f]} m_f \mathrm{tr}(\mathrm{Frob}_q | A_f)$, where the sum is taken over the distinct orbits for $f \in \mathcal{B}$.

Example 4.6. We compute the number of points of $X(1, 163, 1, 1, 1, 1) = X_0^+(163)$ over $\mathbb{F}_{2^2}$ without using the explicit equation in [19]. Consider the space of cusp forms $\mathcal{S}_2^{\mathrm{new}}(\Gamma_0(163))$. This space has dimension 13 and let f_1, f_2, f_3 be representatives under the Galois action. The class of f_1 has just one element, the class of f_2 has 5 elements and the class of f_3 has 7 elements. Since f_3 has negative eigenvalue, its class is discarded.

We compute $m_{f_1} = m_{f_2} = 1$, hence the genus of $X_0^+(163)$ is 6. The Hecke eigenvalues are $a_2(f_1) = 0$ and $a_2(h) \approx -2.711, -2.484, -1.634, 0.163, 1.666$, for $h \in [f_2]$. We consider the polynomial $(x^2 - a_2(f_1)x+2)\prod_{h\in[f_2]}(x^2-a_2(h)x+2)$. We denote its roots by α_j and β_j, where $\alpha_1 \approx 1.414i$, $\alpha_2 \approx -1.355+0.402i$, $\alpha_3 \approx -1.242+0.675i$, $\alpha_4 \approx -0.817+1.154i$, $\alpha_5 \approx 0.081 + 1.411i$, $\alpha_6 \approx 0.833 + 1.1425i$ and $\beta_j = \bar{\alpha}_j$ is the complex conjugated of α_j. Hence $\#X_0^+(163)(\mathbb{F}_{2^2}) = 4 + 1 - \sum_{j=1}^{6}(\alpha_j^2 + \beta_j^2) = 4 + 1 + 5 = 10$.

Example 4.7. We compute the number of points of $X(1, 17, 1, 1, 1, 3)$ over $\mathbb{F}_2$. We have to consider the space of cusp forms $\mathcal{S}_2^{\text{new}}(\Gamma_0(D))$ at levels $D = 1, 9, 17, 153$. The first two spaces are trivial. The third one has dimension 1, but the corresponding representative under the Galois action must be discarded, since the eigenvalue of Atkin-Lehner operator w_{17} is -1. Finally, the last space has 5 representatives under the Galois action and we denote them by f_1, f_2, f_3, f_4, f_5. Four of these classes should be discarded since they have at least a negative eigenvalue. We denote by f the unique representative whose both eigenvalues of w_3 and w_{17} are positive. Then A_f has dimension 1 and $m_f = \sigma_0(1)\sigma_0^*(1) = 1$, so it follows that the genus of $X(1, 17, 1, 1, 1, 3)$ must be 1. The eigenvalue of T_2 acting on f is $a_2(f) = -2$. Then $\#X(1, 17, 1, 1, 1, 3)(\mathbb{F}_2) = 2 + 1 + 2 = 5$. This is the maximum possible value for an elliptic curve over $\mathbb{F}_2$ according to [30].

Example 4.8. We compute the number of points of $X(5, 3, 1, 1, 2, 1)$ over $\mathbb{F}_{7^2}$. We have to consider the space of cusp forms $\mathcal{S}_2^{\text{new}}(\Gamma_0(D))$ at levels $D = 1, 3, 4, 5, 12, 15, 20, 60$. Only the spaces corresponding to $D = 15$ and $D = 20$ are non-trivial, more precisely, $\mathcal{S}_2^{\text{new}}(\Gamma_0(D))$ has dimension 1 in both these cases. We denote by f_1 and f_2, respectively, the corresponding representative under the Galois action. In both cases, the action under the Atkin-Lehner involution w_3 gives positive eigenvalues so both f_1 and f_2 must be considered. Since $m_{f_1} = \sigma_0(1)\sigma_0^*(1) = 1$ and $m_{f_2} = \sigma_0(1)\sigma_0^*(3) = 1$, it follows that $X(5, 3, 1, 1, 2, 1)$ has genus 2. The eigenvalue of T_7 acting on f_1 and f_2 are 0 and 2, respectively. Denote by $\alpha_1, \beta_1, \alpha_2, \beta_2$ the roots of the polynomial $(x^2 + 7)(x^2 - 2x + 7)$. Then $\alpha_1 \approx 2.646i$, $\beta_1 \approx -2.646i$, $\alpha_2 \approx 1 + 2.499i$, $\beta_2 \approx 1 - 2.499i$ and $\#X(5, 3, 1, 1, 2, 1)(\mathbb{F}_{7^2}) = 7^2 + 1 - \sum_{i=1}^{2}(\alpha_i^2 + \beta_i^2) = 49 + 1 + 24 = 74$.

5. Asymptotic estimates

In this section we estimate the number of points on the reductions over prime finite fields of the curves $X = X(n_0, n_{0^+}, n_{\text{s}}, n_{\text{s}^+}, n_{\text{ns}}, n_{\text{ns}^+})$. We start by recalling a classical formula which we then combine with estimates on the trace of Hecke operators. Notice that by Theorem 3.8, the space of regular differentials on X can be identified with a direct sum of spaces of newforms of shape $\mathcal{S}_2^{\text{new}}(\Gamma_0(d))^W$ for W a certain group of Atkin-Lehner operators and d a suitable positive integer. In particular, this decomposition defines an action of Hecke operators on $\Omega^1_{X/\mathbb{C}}$.

Proposition 5.1. *Given $X = X(n_0, n_{0^+}, n_{\mathrm{s}}, n_{\mathrm{s}^+}, n_{\mathrm{ns}}, n_{\mathrm{ns}^+})$ and defining $T_{p^{-1}} := 0$, we have*

$$\#X(\mathbb{F}_{p^e}) = p^e + 1 - \operatorname{tr}(T_{p^e}|\Omega^1_{X/\mathbb{C}}) + p\operatorname{tr}(T_{p^{e-2}}|\Omega^1_{X/\mathbb{C}}),$$

for each integer $e \geqslant 1$ and for every prime p not dividing $n = n_0 n_{0^+} n_{\mathrm{s}} n_{\mathrm{s}^+} n_{\mathrm{ns}} n_{\mathrm{ns}^+}$.

Proof. Let $\alpha_1, \dots, \alpha_g, \beta_1, \dots, \beta_g$ be the eigenvalues of the Frobenius acting on the Tate module of the Jacobian of $X_{\mathbb{F}_p}$. By Proposition 4.4, up to reordering, we can suppose that $\alpha_i + \beta_i = a_p(f_i)$, where $f_1, \dots, f_g$ are the normalized eigenforms giving a basis of $\Omega^1_{X/\mathbb{C}}$. Hence because of Equation (4.1) and Proposition 4.4, it is enough to prove that

$$\alpha_i^e + \beta_i^e = a_{p^e}(f_i) - p a_{p^{e-2}}(f_i). \tag{5.2}$$

The case $e = 1$ is true defining $a_{p^{-1}} := 0$. Since $\alpha_i \beta_i = p$ (by Proposition 4.4), and $T_{p^2} = T_p^2 - p$ (by [14, Equation (5.10)]), we have

$$a_{p^2}(f_i) - p = a_p(f_i)^2 - 2p = (\alpha_i + \beta_i)^2 - 2\alpha_i\beta_i = \alpha_i^2 + \beta_i^2,$$

which proves the case $e = 2$. For the inductive step we recall that on $\Omega^1_{X/\mathbb{C}}$ we have

$$T_{p^e} - pT_{p^{e-2}} = T_p(T_{p^{e-1}} - pT_{p^{e-3}}) - p(T_{p^{e-2}} - pT_{p^{e-4}}).$$

Hence, supposing that Equation (5.2) holds for $e-1$ and $e-2$, we get

$$\begin{aligned} a_{p^e}(f_i) - p a_{p^{e-2}}(f_i) &= a_p(f_i)(a_{p^{e-1}}(f_i) - p a_{p^{e-3}}(f_i)) - p(a_{p^{e-2}}(f_i) - p a_{p^{e-4}}(f_i)) \\ &= (\alpha_i + \beta_i)(\alpha_i^{e-1} + \beta_i^{e-1}) - (\alpha_i\beta_i)(\alpha_i^{e-2} + \beta_i^{e-2}) = \alpha_i^e + \beta_i^e. \quad \square \end{aligned}$$

To estimate the traces of Hecke operators on $\mathcal{S}_2^{\mathrm{new}}(\Gamma_0(d))^W$ for W a group of Atkin-Lehner operators, it is enough to estimate $\operatorname{tr}(T_p w_m|\mathcal{S}_2^{\mathrm{new}}(\Gamma_0(d)))$ for each $w_m \in W$. A small remark on notation: given the prime factorization $d = p_1^{e_2} \cdots p_r^{e_r}$, here and in Section 3, we sometimes write w_{p_i} meaning $w_{p_i^{e_i}}$, while other times we use the usual notation w_m for $m \mid d$ such that $\gcd(m, d/m) = 1$. To estimate the trace of $T_k w_m$, for such a divisor m of d, we look at [7, Proposition 2.8], which states:

$$|\operatorname{tr}(T_k w_m|\mathcal{S}_2^{\mathrm{new}}(\Gamma_0(d))) - \delta(\sqrt{k} \in \mathbb{Z})F(d, m)| < c_0(k + \sqrt{kd})\sigma_0^3(d)\sigma_0(k)\log^2(4kd), \tag{5.3}$$

where c_0 is an absolute constant, σ_0 is the function counting the number of divisors of a natural number, $\delta(\text{condition})$ is 1 if the condition is true and 0 otherwise, and

$$F(d, m) := \mu(\sqrt{m})\frac{d}{m} \prod_{\ell \in \mathcal{P}(\frac{d}{m})} \Big(1 - \frac{1}{\ell} - \frac{\delta(\ell^2|\frac{d}{m})}{\ell^2} + \frac{\delta(\ell^3|\frac{d}{m})}{\ell^3}\Big),$$

with $\mathcal{P}(N)$ the set of prime divisors of an integer N, and μ the Möebius function extended so that $\mu(\sqrt{m}) = 0$ if $\sqrt{m}$ is not an integer. Combining Equation (5.3) and Proposition 5.1 we get the following proposition.

Proposition 5.4. *There exists an absolute constant C such that, for each curve $X = X(n_0, n_{0^+}, n_{\mathrm{s}}, n_{\mathrm{s}^+}, n_{\mathrm{ns}}, n_{\mathrm{ns}^+})$ of genus g and for each prime power $q = p^e$ coprime to $n_0 n_{0^+} n_{\mathrm{s}} n_{\mathrm{s}^+} n_{\mathrm{ns}} n_{\mathrm{ns}^+}$, we have*

$$\begin{cases} \#X(\mathbb{F}_q) < C(q + \sqrt{gq}) g^{\frac{10}{\log\log g}} p \log^3 q, & \text{if } q \text{ is not a square,} \\ |\#X(\mathbb{F}_q) - (p-1)g| < C(q + \sqrt{gq}) g^{\frac{10}{\log\log g}} p \log^3 q, & \text{if } q \text{ is a square.} \end{cases}$$

Proof. We start by slightly simplifying Equation (5.3): using [24, Theorem 1] to bound σ_0, we get

$$|\mathrm{tr}(w_m | \mathcal{S}_2^{\mathrm{new}}(\Gamma_0(d))) - F(d, m)| < 2c_0 d^{\frac{1}{2} + \frac{4.4}{\log\log d}} \tag{5.5}$$

when specializing to $k = 1$ in Equation (5.3); while for $k = r$ a prime power we have

$$|\mathrm{tr}(T_r w_m | \mathcal{S}_2^{\mathrm{new}}(\Gamma_0(d))) - \delta(\sqrt{r} \in \mathbb{Z}) F(d, m)| < 20 c_0 d^{\frac{4.4}{\log\log d}} (r + \sqrt{rd}) \log^3 r. \tag{5.6}$$

Since we are only interested in the cases where $\mathcal{S}_2^{\mathrm{new}}(\Gamma_0(d)) \neq 0$, we restrict to the cases $d \geqslant 11$, hence $\log\log d$ makes sense and is positive.

We recall that, for each finite group G acting on a finite vector space V, the linear operator $\sum_{g \in G} g \colon V \to V$ has trace equal to $\#G \dim(V^G)$. Hence, applying Equation (5.5), for each group of the form $W = \langle w_\ell : \ell \in \mathcal{Q} \rangle$ with $\mathcal{Q}$ a subset of the prime divisors of d, we can write

$$\dim(J_0(d)^W) = \frac{1}{\#W} \sum_{w_m \in W} \mathrm{tr}(w_m | \mathcal{S}_2^{\mathrm{new}}(\Gamma_0(d))) = F(d, W) + \epsilon(d, W), \tag{5.7}$$

where $|\epsilon(d, W)| < 2c_0 d^{\frac{1}{2} + \frac{4.4}{\log\log d}}$ and $F(d, W)$ is defined and can be estimated as follows

$$F(d, W) := \frac{1}{\#W} \sum_{w_m \in W} F(d, m) = \frac{1}{\#W} \sum_{\{\ell_1, \dots, \ell_r\} \subseteq \mathcal{Q}} F(d, \ell_1^{e_{\ell_1}} \cdots \ell_r^{e_{\ell_r}}) =$$

$$= \frac{d}{\#W} \sum_{\{\ell_1, \dots, \ell_r\} \subseteq \mathcal{Q}} \prod_{\ell \in \{\ell_1, \dots, \ell_r\}} \frac{\mu(\ell^{e_\ell/2})}{\ell^{e_\ell}} \prod_{\substack{\ell | d \\ \ell \notin \{\ell_1, \dots, \ell_r\}}} \left(1 - \frac{1}{\ell} - \frac{\delta(\ell^2 | \frac{d}{m})}{\ell^2} + \frac{\delta(\ell^3 | \frac{d}{m})}{\ell^3}\right) =$$

$$= \frac{d}{\#W} \prod_{\substack{\ell | d \\ \ell \notin \mathcal{Q}}} \left(1 - \frac{1}{\ell} - \frac{\delta(\ell^2 | \frac{d}{m})}{\ell^2} + \frac{\delta(\ell^3 | \frac{d}{m})}{\ell^3}\right) \cdot$$

$$\cdot \sum_{\{\ell_1, \dots, \ell_r\} \subseteq \mathcal{Q}} \prod_{\ell \in \{\ell_1, \dots, \ell_r\}} \frac{\mu(\ell^{e_\ell/2})}{\ell^{e_\ell}} \prod_{\substack{\ell \in \mathcal{Q} \\ \ell \notin \{\ell_1, \dots, \ell_r\}}} \left(1 - \frac{1}{\ell} - \frac{\delta(\ell^2 | \frac{d}{m})}{\ell^2} + \frac{\delta(\ell^3 | \frac{d}{m})}{\ell^3}\right) =$$

$$= \frac{d}{\#W} \prod_{\substack{\ell | d \\ \ell \notin \mathcal{Q}}} \Big(1 - \frac{1}{\ell} - \frac{\delta(\ell^2|\frac{d}{m})}{\ell^2} + \frac{\delta(\ell^3|\frac{d}{m})}{\ell^3}\Big) \cdot$$

$$\cdot \prod_{\ell \in \mathcal{Q}} \Big(1 - \frac{1}{\ell} - \frac{\delta(\ell^2|\frac{d}{m})}{\ell^2} + \frac{\delta(\ell^3|\frac{d}{m})}{\ell^3} + \frac{\mu(\ell^{e_\ell/2})}{\ell^{e_\ell}}\Big) \geqslant$$

$$\geqslant \frac{d}{\sigma_0(d)} \prod_{\ell | d} (1 - \frac{1}{\ell})(1 - \frac{1}{\ell^2})^2 \geqslant \frac{\varphi(d)}{\sigma_0(d)} \zeta(2)^{-2} \geqslant c_1 d^{1 - \frac{1.2}{\log\log d}},$$

where φ is the Euler's totient function, estimated as in [17, Theorem 327], and ζ is the Riemann zeta function. Analogously, Equation (5.6) implies that

$$\begin{aligned} \mathrm{tr}(T_r | \mathcal{S}_2^{\mathrm{new}}(\Gamma_0(d))^W) &= \frac{1}{\#W} \sum_{w_m \in W} \mathrm{tr}(T_r w_m | \mathcal{S}_2^{\mathrm{new}}(\Gamma_0(d))) = \\ &= \delta(\sqrt{r} \in \mathbb{Z}) F(d, W) + \epsilon(d, W, r), \end{aligned} \tag{5.8}$$

with $|\epsilon(d, W, r)| < 20 c_0 d^{\frac{4.4}{\log\log d}} (r + \sqrt{rd}) \log^3 r$.

We now look at the curve X. Using Theorem 3.8 to write $\Omega^1_{X/\mathbb{C}}$ as a sum of spaces of the form $\mathcal{S}_2^{\mathrm{new}}(\Gamma_0(d))^W$ and taking linear combinations of Equations (5.8) and (5.7), we get

$$g = F + \epsilon, \qquad \mathrm{tr}(T_r | \Omega^1_{X/\mathbb{C}}) = \delta(\sqrt{r} \in \mathbb{Z}) F + \epsilon_r, \tag{5.9}$$

for

$$F = \sum_d \sigma_0\Big(\frac{n_0 n_{\mathrm{s}}^2}{d_0 d_{\mathrm{s}}}\Big) \sum_{m^2 || \frac{n_{0^+} n_{\mathrm{s}^+}^2}{d_{0^+} d_{\mathrm{s}^+}}} \sigma_0^+\Big(\frac{n_{0^+} n_{\mathrm{s}^+}^2}{d_{0^+} d_{\mathrm{s}^+} m^2}\Big) F\Big(d_0 d_{0^+} d_{\mathrm{s}} d_{\mathrm{s}^+} d_{\mathrm{ns}}^2 d_{\mathrm{ns}^+}^2, \langle w_\ell : \ell | m d_{\mathrm{ns}^+} \rangle\Big),$$

$$\epsilon = \sum_d \sigma_0\Big(\frac{n_0 n_{\mathrm{s}}^2}{d_0 d_{\mathrm{s}}}\Big) \sum_{m^2 || \frac{n_{0^+} n_{\mathrm{s}^+}^2}{d_{0^+} d_{\mathrm{s}^+}}} \sigma_0^+\Big(\frac{n_{0^+} n_{\mathrm{s}^+}^2}{d_{0^+} d_{\mathrm{s}^+} m^2}\Big) \epsilon\Big(d_0 d_{0^+} d_{\mathrm{s}} d_{\mathrm{s}^+} d_{\mathrm{ns}}^2 d_{\mathrm{ns}^+}^2, \langle w_\ell : \ell | m d_{\mathrm{ns}^+} \rangle\Big),$$

$$\epsilon_r = \sum_d \sigma_0\Big(\frac{n_0 n_{\mathrm{s}}^2}{d_0 d_{\mathrm{s}}}\Big) \sum_{m^2 || \frac{n_{0^+} n_{\mathrm{s}^+}^2}{d_{0^+} d_{\mathrm{s}^+}}} \sigma_0^+\Big(\frac{n_{0^+} n_{\mathrm{s}^+}^2}{d_{0^+} d_{\mathrm{s}^+} m^2}\Big) \epsilon\Big(d_0 d_{0^+} d_{\mathrm{s}} d_{\mathrm{s}^+} d_{\mathrm{ns}}^2 d_{\mathrm{ns}^+}^2, \langle w_\ell : \ell | m d_{\mathrm{ns}^+} \rangle, r\Big),$$

where the external sums are indexed over d equal to the product of $d_0, d_{0^+}, d_{\mathrm{s}}, d_{\mathrm{s}^+}, d_{\mathrm{ns}}, d_{\mathrm{ns}^+}$, which vary across the divisors respectively of $n_0, n_{0^+}, n_{\mathrm{s}}^2, n_{\mathrm{s}^+}^2, n_{\mathrm{ns}}, n_{\mathrm{ns}^+}$, while the internal sums of the form $\sum_{m^2||k}$ are indexed over the positive integers m such that m^2 divides k and $\gcd(k, \frac{k}{m^2}) = 1$, and finally σ_0^+ is the multiplicative function such that $\sigma_0^+(\ell^e) = \lceil \frac{e}{2} \rceil$ for each prime power ℓ^e. Under the notation $N = n_0 n_{0^+} n_{\mathrm{s}}^2 n_{\mathrm{s}^+}^2 n_{\mathrm{ns}}^2 n_{\mathrm{ns}^+}^2$, using [24, Theorem 1] and the previous estimates on $F(d, W)$, $\epsilon(d, W)$ and $\epsilon(d, W, r)$, we get

$$F \geqslant F(N, \langle w_\ell : \ell | n_{\mathrm{ns}^+} \rangle) \geqslant c_1 N^{1-\frac{1.2}{\log\log N}},$$
$$|\epsilon| \leqslant \sigma_0(N)^3 \max\{|\epsilon(d,W)| : d|N, W < \langle w_\ell : \ell | d \rangle\} < 2c_0 N^{\frac{1}{2}+\frac{7.6}{\log\log N}},$$
$$|\epsilon_r| \leqslant \sigma_0(N)^3 \max\{\epsilon(d,W,r) : d|N, W < \langle w_\ell : \ell | d \rangle\} \leqslant 20c_0 N^{\frac{7.6}{\log\log N}}(r+\sqrt{rN})\log^3 r.$$

Plugging the first two bounds above into Equation (5.9), for appropriate constants c_2 and c_3, we have

$$g > c_2 N^{1-\frac{1.2}{\log\log N}}$$

that implies

$$N < c_3 g^{1+\frac{1.4}{\log\log g}}.$$

Again using Equation (5.9) and the bounds on ϵ, ϵ_r, we get, for a suitable c_4, that

$$\begin{aligned} |\mathrm{tr}(T_r|\Omega^1_{X/\mathbb{C}}) - \delta(\sqrt{r}\in\mathbb{Z})g| &= |\epsilon_r - \delta(\sqrt{r}\in\mathbb{Z})\epsilon| \\ &< 2c_0 N^{\frac{1}{2}+\frac{7.6}{\log\log N}} + 20c_0 N^{\frac{7.6}{\log\log N}}(r+\sqrt{rN})\log^3 r \\ &< c_4(r+\sqrt{r}g^{\frac{1}{2}+\frac{0.7}{\log\log g}})g^{\frac{8.4}{\log\log g}}\log^3 r. \end{aligned}$$

This estimate, together with Proposition 5.1, implies the desired result. □

The above proposition implies that, for a fixed q, we expect a large number of points on our curves mostly for $q = p^2$. Anyway, the estimates are only relevant for N large with respect to q, and indeed we found records also for fields of the form p^5.

Remark 5.10. As first shown in [25] (see also [28, Section 1] or [6, Section 3.3]), the case $q = p^2$ is known to provide many rational points in modular curves, thanks to the presence of supersingular points: the j-invariant of a supersingular elliptic curve E lies in $\mathbb{F}_{p^2}$ and, up to twisting, the absolute Galois of $\mathbb{F}_{p^2}$ acts diagonally on the torsion of E. For example, the bounds in [6, Lemma 3.20] imply that, for each congruence subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$, and for each prime p coprime to the level, we have

$$X_\Gamma(\mathbb{F}_{p^2}) > (p-1)(g_\Gamma - 1), \tag{5.11}$$

where g_Γ is the genus of X_Γ. This inequality can easily be extended to our curves. Indeed, let $X = X(n_0, n_{0^+}, n_{\mathrm{s}}, n_{\mathrm{s}^+}, n_{\mathrm{ns}}, n_{\mathrm{ns}^+})$, with genus g and let p be a prime not dividing $n_0 n_{0^+} n_{\mathrm{s}} n_{\mathrm{s}^+} n_{\mathrm{ns}} n_{\mathrm{ns}^+}$. Then we can write $X = X_\Gamma/G$ for a suitable choice of Γ and of a group of automorphisms G. The Riemann-Hurwitz's formula implies that g satisfies $g-1 \leqslant (g_\Gamma - 1)/(\#G)$. The inclusion $X(\mathbb{F}_{p^2}) \supset X_\Gamma(\mathbb{F}_{p^2})/G$, together with orbit counting implies that $X(\mathbb{F}_{p^2})$ has cardinality at least $\#X_\Gamma(\mathbb{F}_{p^2})/\#G$. Using also Equation (5.11) we get $X(\mathbb{F}_{p^2}) > (p-1)(g-1)$.

6. Greatest hits

We implemented Algorithm 4.5 and applied it to all the curves for which we could compute the number of points using the numerical data available at [18]. In Table 6.1 and Table 6.2 we list all the improved bounds, which we found, for the number of points of $X(n_0, n_{0^+}, n_{\mathrm{ns}}, n_{\mathrm{ns}^+})$ over $\mathbb{F}_q$, where $n_0 n_{0^+} n_{\mathrm{ns}}^2 n_{\mathrm{ns}^+}^2 \leqslant 10000$ and $q = p^k$ is a prime power with $p < 20$ and $k \leqslant 5$. As explained in Remark 2.4, the search along this set of curves gives the same results over the bigger set of $X(n_0, n_{0^+}, n_{\mathrm{s}}, n_{\mathrm{s}^+}, n_{\mathrm{ns}}, n_{\mathrm{ns}^+})$ curves since

$$\#X(n_0, n_{0^+}, n_{\mathrm{s}}, n_{\mathrm{s}^+}, n_{\mathrm{ns}}, n_{\mathrm{ns}^+})(\mathbb{F}_q) = \#X(n_0 n_{\mathrm{s}}^2, n_{0^+} n_{\mathrm{s}^+}^2, 1, 1, n_{\mathrm{ns}}, n_{\mathrm{ns}^+})(\mathbb{F}_q).$$

The entries list the genus g of the curve, the size q of the finite field, the 4-tuple $(n_0, n_{0^+}, n_{\mathrm{ns}}, n_{\mathrm{ns}^+})$ and the number $\#X(\mathbb{F}_q)$ of $\mathbb{F}_q$-points of $X(n_0, n_{0^+}, n_{\mathrm{ns}}, n_{\mathrm{ns}^+})$. When a lower bound $L_g(\mathbb{F}_q)$ is not yet available, we list a curve of genus g with M points only if the corresponding upper bound satisfies $M_g(\mathbb{F}_q) < q+1+\sqrt{2}(M-q-1)$, as it is done in the database [30] at the time of writing (September 2022).

Table 6.1
Improved bounds of the form $\#X(n_0, n_{0^+}, n_{\mathrm{ns}}, n_{\mathrm{ns}^+})(\mathbb{F}_q)$ for $n_0 n_{0^+} n_{\mathrm{ns}}^2 n_{\mathrm{ns}^+}^2 \leqslant 10000$ and $g \leqslant 25$.

g	q	$(n_0, n_{0^+}, n_{\mathrm{ns}}, n_{\mathrm{ns}^+})$	$\#X(\mathbb{F}_q)$	g	q	$(n_0, n_{0^+}, n_{\mathrm{ns}}, n_{\mathrm{ns}^+})$	$\#X(\mathbb{F}_q)$
5	5^2	$(1, 572, 1, 1)$	71	14	13^2	$(7, 19, 1, 3)$	442
6	3^2	$(1, 398, 1, 1)$	37	15	7^2	$(1, 956, 1, 1)$	214
7	11^5	$(1, 12, 1, 7)$	166589	15	13^5	$(27, 14, 1, 1)$	384496
8	13^2	$(1, 4, 9, 1)$	364	15	17^5	$(1, 80, 3, 1)$	1445778
9	3^5	$(5, 17, 2, 1)$	464	16	11^2	$(9, 1, 1, 7)$	414
9	7^5	$(99, 1, 1, 1)$	18968	16	11^5	$(3, 4, 1, 7)$	172432
9	11^3	$(4, 43, 1, 1)$	1812	17	13^2	$(7, 3, 1, 8)$	500
9	11^5	$(8, 39, 1, 1)$	167544	18	3^2	$(1, 878, 1, 1)$	73
9	13^5	$(96, 1, 1, 1)$	382096	18	7^2	$(1, 179, 1, 4)$	224
9	17^5	$(41, 4, 1, 1)$	1438108	18	17^2	$(1, 271, 1, 3)$	746
10	5^5	$(1, 668, 1, 1)$	4092	19	2^2	$(225, 1, 1, 1)$	38
10	11^5	$(3, 104, 1, 1)$	168744	19	13^2	$(4, 1, 9, 1)$	582
10	13^5	$(27, 7, 1, 1)$	382887	20	3^2	$(1, 1244, 1, 1)$	80
10	19^5	$(92, 1, 1, 1)$	2499156	20	17^2	$(8, 13, 1, 3)$	862
11	7^2	$(1, 764, 1, 1)$	176	21	11^2	$(256, 1, 1, 1)$	464
11	17^5	$(104, 1, 1, 1)$	1438748	21	17^2	$(45, 1, 1, 4)$	824
11	19^5	$(17, 4, 1, 3)$	2501908	22	2^2	$(1, 761, 1, 1)$	43
12	3^2	$(4, 7, 1, 5)$	58	22	3^2	$(121, 4, 1, 1)$	80
12	5^2	$(16, 13, 1, 1)$	122	22	13^2	$(12, 25, 1, 1)$	594
12	11^2	$(12, 13, 1, 1)$	338	23	5^2	$(1, 887, 1, 1)$	180
12	7^2	$(1, 718, 1, 1)$	171	23	13^2	$(3, 476, 1, 1)$	594
12	11^5	$(12, 13, 1, 1)$	170676	23	19^2	$(3, 1, 14, 1)$	988
12	19^5	$(16, 13, 1, 1)$	1445778	24	5^2	$(1, 412, 1, 3)$	188
13	5^2	$(4, 143, 1, 1)$	126	24	11^2	$(9, 2, 1, 7)$	498
13	7^2	$(1, 599, 1, 1)$	184	24	17^2	$(1, 981, 1, 1)$	880
13	13^2	$(9, 1, 1, 8)$	456	25	5^2	$(4, 167, 1, 1)$	204
13	17^2	$(144, 1, 1, 1)$	696	25	13^2	$(180, 1, 1, 1)$	672
14	3^2	$(1, 734, 1, 1)$	59	25	17^2	$(49, 1, 2, 3)$	990
14	7^2	$(1, 734, 1, 1)$	194	25	11^5	$(24, 13, 1, 1)$	180048

Table 6.2
Improved bounds of the form $\#X(n_0, n_{0^+}, n_{\rm ns}, n_{\rm ns^+})(\mathbb{F}_q)$ for $25 < g \leqslant 50$.

g	q	$(n_0, n_{0^+}, n_{\rm ns}, n_{\rm ns^+})$	$\#X(\mathbb{F}_q)$	g	q	$(n_0, n_{0^+}, n_{\rm ns}, n_{\rm ns^+})$	$\#X(\mathbb{F}_q)$
27	5^2	$(1, 1509, 1, 1)$	191	36	5^2	$(1, 2327, 1, 1)$	236
27	11^2	$(9, 76, 1, 1)$	584	36	5^2	$(4, 79, 1, 3)$	243
28	5^2	$(1, 1336, 1, 1)$	200	37	19^2	$(9, 1, 2, 7)$	1452
29	2^2	$(1, 1091, 1, 1)$	55	38	3^2	$(1, 1231, 1, 1)$	131
29	5^2	$(1, 2004, 1, 1)$	200	38	17^2	$(1, 416, 1, 3)$	1224
29	17^2	$(99, 4, 1, 1)$	1000	39	5^2	$(1, 1774, 1, 1)$	260
29	19^2	$(99, 4, 1, 1)$	1216	40	3^2	$(1, 1756, 1, 1)$	142
30	3^2	$(1, 1375, 1, 1)$	99	40	5^2	$(1, 1559, 1, 1)$	264
30	13^2	$(8, 61, 1, 1)$	730	41	5^2	$(3, 83, 1, 4)$	256
30	19^2	$(8, 61, 1, 1)$	1202	41	11^2	$(128, 1, 1, 3)$	880
31	5^2	$(1, 1532, 1, 1)$	228	42	3^2	$(1, 1279, 1, 1)$	132
31	13^2	$(81, 7, 1, 1)$	744	42	5^2	$(1, 2012, 1, 1)$	296
31	17^2	$(4, 455, 1, 1)$	1038	43	5^2	$(3, 623, 1, 1)$	266
31	19^2	$(9, 1, 7, 1)$	1260	43	7^2	$(9, 43, 2, 1)$	444
31	13^5	$(27, 28, 1, 1)$	398892	44	3^2	$(1, 1966, 1, 1)$	136
32	3^2	$(1, 1039, 1, 1)$	112	44	5^2	$(1, 1487, 1, 1)$	289
32	5^2	$(1, 542, 1, 3)$	213	45	3^2	$(1, 1399, 1, 1)$	145
32	19^2	$(11, 140, 1, 1)$	1236	45	5^2	$(1, 1427, 1, 1)$	275
33	5^2	$(1, 1319, 1, 1)$	225	46	5^2	$(4, 263, 1, 1)$	306
34	3^2	$(1, 1678, 1, 1)$	113	47	2^2	$(1, 2681, 1, 1)$	74
34	5^2	$(1, 1223, 1, 1)$	241	47	5^2	$(3, 383, 1, 1)$	298
34	13^2	$(9, 100, 1, 1)$	798	48	5^2	$(1, 796, 1, 3)$	302
34	17^2	$(16, 1, 1, 7)$	1260	48	13^2	$(9, 97, 1, 1)$	1058
34	11^5	$(12, 1, 1, 7)$	180450	49	5^2	$(4, 311, 1, 1)$	315
35	3^2	$(1, 1916, 1, 1)$	122	50	5^2	$(1, 2396, 1, 1)$	306
35	5^2	$(1, 1916, 1, 1)$	242	50	7^2	$(1, 2396, 1, 1)$	506
36	3^2	$(4, 199, 1, 1)$	130	50	19^2	$(9, 146, 1, 1)$	1750

Data availability

Data will be made available on request.

Appendix A. More data

In Tables A.1, A.2, A.3, A.4, A.5, A.6, A.7 and A.8, we list the maximal values that we found for the number of points of the curves $X(n_0, n_{0^+}, n_{\rm ns}, n_{\rm ns^+})$ over $\mathbb{F}_q$, for $n_0 n_{0^+} n_{\rm ns}^2 n_{\rm ns^+}^2 \leqslant 10000$ and $q = p^k$ a prime power with $p < 20$, $k \leqslant 5$ for p odd and $k \leqslant 6$ for $p = 2$. As in Section 6 we restrict our search to the curves $X(n_0, n_{0^+}, n_{\rm ns}, n_{\rm ns^+})$. The entries are of the type $(n_0, n_{0^+}, n_{\rm ns}, n_{\rm ns^+}) \to \#X(n_0, n_{0^+}, n_{\rm ns}, n_{\rm ns^+})(\mathbb{F}_q)$ and the field is indicated only once at the top of the column. All the values that improve previous known lower bounds $L_g(\mathbb{F}_q)$ are in bold. When a lower bound $L_g(\mathbb{F}_q)$ is not yet available, we display in bold curves with M points only if the corresponding upper bound satisfies $M_g(\mathbb{F}_q) < q + 1 + \sqrt{2}(M - q - 1)$, as it is done in the database [30] at the time of writing (September 2022).

Table A.1
Table for $\max\{\#X(n_0, n_{0^+}, n_{\mathrm{ns}}, n_{\mathrm{ns}^+})(\mathbb{F}_q)\}$ with $q = 2^k$ and $n_0 n_{0^+} n_{\mathrm{ns}}^2 n_{\mathrm{ns}^+}^2 \leqslant 10000$.

g	$\mathbb{F}_2$	$\mathbb{F}_{2^2}$	$\mathbb{F}_{2^3}$	$\mathbb{F}_{2^4}$	$\mathbb{F}_{2^5}$	$\mathbb{F}_{2^6}$
1	(1, 17, 1, 3)→5	(1, 1, 1, 11)→9	(1, 5, 3, 1)→14	(1, 17, 1, 3)→25	(1, 11, 1, 3)→44	(1, 1, 1, 11)→81
2	(1, 67, 1, 1)→6	(1, 29, 1, 3)→10	(5, 7, 1, 1)→16	(1, 1, 9, 1)→31	(1, 13, 3, 1)→51	(1, 3, 1, 7)→91
3	(1, 97, 1, 1)→7	(1, 17, 1, 5)→14	(1, 175, 1, 1)→16	(7, 13, 1, 1)→33	(1, 11, 3, 1)→63	(7, 15, 1, 1)→103
4	(1, 47, 1, 3)→7	(1, 7, 1, 15)→15	(7, 17, 1, 1)→16	(13, 7, 1, 1)→32	(5, 29, 1, 1)→53	(1, 1, 5, 3)→119
5	(1, 157, 1, 1)→8	(1, 645, 1, 1)→17	(3, 1, 1, 7)→17	(1, 555, 1, 1)→33	(13, 1, 3, 1)→62	(3, 1, 1, 7)→117
6	(1, 223, 1, 1)→9	(1, 447, 1, 1)→19	(1, 9, 1, 7)→17	(3, 37, 1, 1)→45	(1, 297, 1, 1)→66	(9, 13, 1, 1)→143
7	(1, 193, 1, 1)→8	(1, 5, 1, 11)→20	(15, 11, 1, 1)→16	(5, 27, 1, 1)→39	(1, 423, 1, 1)→56	(1, 9, 5, 1)→110
8	(1, 427, 1, 1)→10	(1, 545, 1, 1)→22	(25, 7, 1, 1)→25	(1, 333, 1, 1)→43	(31, 5, 1, 1)→64	(5, 1, 1, 9)→113
9	(3, 91, 1, 1)→10	(1, 689, 1, 1)→24	(3, 1, 7, 1)→26	(9, 19, 1, 1)→62	(19, 1, 3, 1)→60	(3, 85, 1, 1)→153
10	(1, 307, 1, 1)→10	(1, 13, 1, 15)→27	(1, 343, 1, 1)→17	(127, 1, 1, 1)→40	(19, 11, 1, 1)→64	(1, 175, 1, 3)→126
11	(1, 313, 1, 1)→11	(1, 717, 1, 1)→25	(5, 7, 3, 1)→24	(1, 1295, 1, 1)→43	(13, 19, 1, 1)→65	(5, 43, 1, 1)→121
12	(3, 73, 1, 1)→11	(3, 131, 1, 1)→29	(3, 73, 1, 1)→17	(1, 513, 1, 1)→56	(1, 47, 3, 1)→59	(1, 765, 1, 1)→143
13	(3, 133, 1, 1)→12	(135, 1, 1, 1)→30	(1, 621, 1, 1)→22	(9, 1, 5, 1)→60	(5, 53, 1, 1)→76	(15, 13, 1, 1)→142
14	(1, 871, 1, 1)→10	(1, 521, 1, 1)→31	(13, 33, 1, 1)→16	(1, 43, 1, 5)→44	(27, 11, 1, 1)→93	(3, 1, 1, 11)→135
15	(1, 433, 1, 1)→13	(1, 879, 1, 1)→33	(1, 9, 7, 1)→26	(3, 185, 1, 1)→61	(1, 79, 3, 1)→72	(9, 31, 1, 1)→170
16	(3, 97, 1, 1)→13	(1, 569, 1, 1)→34	(1, 657, 1, 1)→17	(1, 23, 5, 1)→50	(5, 89, 1, 1)→73	(9, 1, 1, 7)→237
17	(1, 457, 1, 1)→12	(1, 29, 1, 7)→35	(1, 669, 1, 1)→18	(65, 1, 1, 3)→52	(7, 61, 1, 1)→67	(3, 103, 1, 1)→170
18	(1, 323, 1, 3)→12	(1, 1077, 1, 1)→36	(71, 1, 1, 3)→16	(9, 37, 1, 1)→83	(9, 47, 1, 1)→97	(5, 73, 1, 1)→153
19	(1, 973, 1, 1)→14	**(225, 1, 1, 1)→38**	(41, 9, 1, 1)→18	(11, 57, 1, 1)→55	(11, 1, 1, 7)→65	(27, 13, 1, 1)→207
20	(1, 1443, 1, 1)→13	(1, 1041, 1, 1)→38	(1, 865, 1, 1)→16	(7, 111, 1, 1)→65	(19, 23, 1, 1)→64	(1, 9, 1, 11)→151
21	(1, 619, 1, 1)→12	(3, 17, 1, 5)→42	(245, 1, 1, 1)→28	(1, 39, 5, 1)→65	(247, 1, 1, 1)→64	(9, 49, 1, 1)→188
22	(1, 577, 1, 1)→16	**(1, 761, 1, 1)→43**	(1, 577, 1, 1)→22	(13, 57, 1, 1)→67	(5, 159, 1, 1)→64	(7, 73, 1, 1)→162
23	(1, 613, 1, 1)→13	(1, 83, 1, 5)→43	(71, 7, 1, 1)→18	(1, 1881, 1, 1)→62	(15, 29, 1, 1)→84	(77, 5, 1, 1)→152
24	(1, 643, 1, 1)→16	(1, 1469, 1, 1)→44	(1, 727, 1, 1)→19	(1, 1665, 1, 1)→67	(7, 89, 1, 1)→76	(1, 1339, 1, 1)→138
25	(1, 1267, 1, 1)→14	(1, 1437, 1, 1)→46	(1, 175, 3, 1)→24	(5, 17, 3, 1)→72	(5, 19, 3, 1)→80	(49, 11, 1, 1)→220
26	(3, 157, 1, 1)→15	(1, 971, 1, 1)→49	(1, 1029, 1, 1)→21	(1, 2373, 1, 1)→56	(7, 195, 1, 1)→72	(9, 85, 1, 1)→199
27	(1, 733, 1, 1)→16	(1, 1383, 1, 1)→49	(1, 1191, 1, 1)→21	(91, 1, 1, 3)→80	(1, 5, 3, 7)→64	(7, 101, 1, 1)→157
28	(1, 787, 1, 1)→15	(1, 941, 1, 1)→52	(25, 7, 1, 3)→25	(27, 19, 1, 1)→108	(1, 1325, 1, 1)→91	(25, 7, 1, 3)→167
29	(1, 757, 1, 1)→15	**(1, 1091, 1, 1)→55**	(19, 5, 3, 1)→26	(295, 1, 1, 1)→58	(173, 3, 1, 1)→65	(7, 155, 1, 1)→164
30	(1, 1263, 1, 1)→16	(1, 231, 1, 5)→51	(1, 1417, 1, 1)→19	(1, 2553, 1, 1)→63	(19, 11, 1, 3)→86	(1, 1, 5, 7)→137
31	(1, 517, 1, 3)→14	(1, 1, 1, 57)→54	(27, 23, 1, 1)→32	(25, 39, 1, 1)→73	(1, 247, 3, 1)→80	(9, 1, 7, 1)→186
32	(1, 1299, 1, 1)→16	(1, 1527, 1, 1)→53	(7, 187, 1, 1)→21	(1, 1, 27, 1)→67	(1, 7, 11, 1)→107	(3, 193, 1, 1)→161
33	(1, 853, 1, 1)→16	(1, 349, 1, 3)→56	(1, 853, 1, 1)→22	(363, 1, 1, 1)→72	(19, 1, 1, 7)→65	(9, 67, 1, 1)→182
34	(1, 937, 1, 1)→16	(1, 1109, 1, 1)→60	(1, 937, 1, 1)→19	(7, 185, 1, 1)→76	(23, 11, 1, 3)→77	(11, 67, 1, 1)→170
35	(1, 1063, 1, 1)→16	(1, 1707, 1, 1)→59	(1, 1389, 1, 1)→22	(119, 1, 1, 3)→88	(7, 19, 3, 1)→80	(25, 31, 1, 1)→270
36	(1, 1413, 1, 1)→15	(1, 2051, 1, 1)→59	(5, 47, 1, 3)→20	(11, 195, 1, 1)→67	(11, 115, 1, 1)→70	(1, 1413, 1, 1)→171
37	(3, 223, 1, 1)→18	(27, 25, 1, 1)→63	(3, 5, 7, 1)→26	(15, 37, 1, 1)→98	(7, 1, 3, 5)→82	(1, 23, 7, 1)→196
38	(1, 1897, 1, 1)→17	(1, 1181, 1, 1)→62	(1, 997, 1, 1)→21	(1, 3219, 1, 1)→74	(121, 7, 1, 1)→69	(7, 113, 1, 1)→161
39	(1, 1497, 1, 1)→17	(1, 409, 1, 3)→65	(1, 1497, 1, 1)→23	(33, 19, 1, 1)→92	(11, 13, 3, 1)→80	(45, 13, 1, 1)→242
40	(1, 353, 1, 3)→20	(1, 1559, 1, 1)→66	(1, 353, 1, 3)→23	(1, 2471, 1, 1)→72	(9, 145, 1, 1)→67	(1, 1, 5, 9)→197
41	(3, 427, 1, 1)→20	(1, 2045, 1, 1)→64	(65, 11, 1, 1)→28	(375, 1, 1, 1)→78	(1, 53, 5, 1)→112	(55, 13, 1, 1)→174
42	(1, 1123, 1, 1)→21	(1, 1361, 1, 1)→73	(1, 1123, 1, 1)→24	(1, 2103, 1, 1)→80	(13, 115, 1, 1)→63	(5, 301, 1, 1)→174
43	(1, 2191, 1, 1)→18	(3, 581, 1, 1)→68	(13, 1, 7, 1)→26	(473, 1, 1, 1)→92	(9, 101, 1, 1)→72	(9, 155, 1, 1)→156
44	(1, 1731, 1, 1)→20	(1, 2105, 1, 1)→66	(1, 1731, 1, 1)→23	(1, 4301, 1, 1)→78	(263, 3, 1, 1)→64	(11, 101, 1, 1)→168
45	(1, 707, 1, 3)→17	(1, 2651, 1, 1)→71	(3, 493, 1, 1)→22	(39, 19, 1, 1)→100	(63, 11, 1, 1)→124	(3, 515, 1, 1)→202
46	(1, 2257, 1, 1)→18	(1, 2229, 1, 1)→72	(1, 1863, 1, 1)→25	(1, 4403, 1, 1)→82	(1, 47, 1, 9)→94	(9, 1, 1, 11)→259
47	(3, 283, 1, 1)→18	**(1, 2681, 1, 1)→74**	(3, 13, 1, 7)→21	(29, 37, 1, 1)→92	(81, 11, 1, 1)→93	(1, 1899, 1, 1)→216
48	(1, 1237, 1, 1)→21	(1, 5, 1, 27)→72	(1, 1237, 1, 1)→27	(3, 629, 1, 1)→96	(1, 803, 1, 3)→57	(5, 193, 1, 1)→201
49	(1, 1857, 1, 1)→19	(1, 1481, 1, 1)→77	(39, 23, 1, 1)→28	(21, 37, 1, 1)→120	(13, 83, 1, 1)→77	(5, 309, 1, 1)→205
50	(1, 1929, 1, 1)→21	(1, 4407, 1, 1)→78	(1, 1929, 1, 1)→24	(1, 5, 1, 23)→82	(29, 65, 1, 1)→73	(1, 93, 5, 1)→206

Table A.2
Table for $\max\{\#X(n_0, n_{0^+}, n_{\mathrm{ns}}, n_{\mathrm{ns}^+})(\mathbb{F}_q)\}$ with $q = 3^k$ and $n_0 n_{0^+} n_{\mathrm{ns}}^2 n_{\mathrm{ns}^+}^2 \leqslant 10000$.

g	$\mathbb{F}_3$	$\mathbb{F}_{3^2}$	$\mathbb{F}_{3^3}$	$\mathbb{F}_{3^4}$	$\mathbb{F}_{3^5}$
1	$(1,37,1,1)\to 7$	$(1,5,1,8)\to 16$	$(1,1,2,5)\to 38$	$(1,7,1,4)\to 96$	$(1,1,1,11)\to 275$
2	$(1,85,1,1)\to 8$	$(1,14,1,5)\to 20$	$(1,11,4,1)\to 44$	$(23,1,1,1)\to 116$	$(1,14,1,5)\to 306$
3	$(4,13,1,1)\to 10$	$(4,31,1,1)\to 28$	$(1,29,2,1)\to 46$	$(1,95,2,1)\to 124$	$(1,136,1,1)\to 304$
4	$(1,148,1,1)\to 11$	$(44,1,1,1)\to 30$	$(1,41,2,1)\to 44$	$(1,160,1,1)\to 138$	$(5,17,1,1)\to 346$
5	$(1,212,1,1)\to 12$	$(1,28,1,5)\to 32$	$(5,44,1,1)\to 52$	$(23,4,1,1)\to 132$	$(1,28,1,5)\to 366$
6	$(1,340,1,1)\to 13$	$\mathbf{(1,398,1,1)\to 37}$	$(1,8,5,1)\to 56$	$(1,272,1,1)\to 142$	$(121,1,1,1)\to 364$
7	$(1,296,1,1)\to 13$	$(4,71,1,1)\to 39$	$(31,4,1,1)\to 54$	$(61,2,1,1)\to 137$	$(4,95,1,1)\to 366$
8	$(1,293,1,1)\to 12$	$(7,13,2,1)\to 42$	$(1,23,4,1)\to 44$	$(101,1,1,1)\to 152$	$(8,17,1,1)\to 364$
9	$(4,37,1,1)\to 16$	$(8,31,1,1)\to 48$	$(1,7,8,1)\to 52$	$(32,5,1,1)\to 176$	$\mathbf{(5,17,2,1)\to 464}$
10	$(1,277,1,1)\to 16$	$(1,755,1,1)\to 47$	$(16,11,1,1)\to 52$	$(4,65,1,1)\to 180$	$(1,191,2,1)\to 383$
11	$(1,317,1,1)\to 15$	$(1,439,1,1)\to 53$	$(104,1,1,1)\to 56$	$(115,1,1,1)\to 164$	$(8,35,1,1)\to 364$
12	$(1,424,1,1)\to 16$	$\mathbf{(4,7,1,5)\to 58}$	$(17,20,1,1)\to 44$	$(1,37,4,1)\to 166$	$(4,7,1,5)\to 484$
13	$(1,373,1,1)\to 18$	$(1,632,1,1)\to 56$	$(20,11,1,1)\to 72$	$(7,32,1,1)\to 168$	$(1,632,1,1)\to 448$
14	$(1,554,1,1)\to 18$	$\mathbf{(1,734,1,1)\to 59}$	$(124,1,1,1)\to 56$	$(61,4,1,1)\to 160$	$(61,5,1,1)\to 344$
15	$(1,113,1,4)\to 17$	$(1,1055,1,1)\to 63$	$(5,29,2,1)\to 50$	$(5,7,4,1)\to 198$	$(161,1,1,1)\to 384$
16	$(1,893,1,1)\to 17$	$(1,796,1,1)\to 70$	$(16,23,1,1)\to 52$	$(16,17,1,1)\to 210$	$(1,305,2,1)\to 414$
17	$(1,634,1,1)\to 19$	$(1,92,1,5)\to 64$	$(5,88,1,1)\to 64$	$(1,592,1,1)\to 172$	$(7,4,1,5)\to 448$
18	$(1,692,1,1)\to 20$	$\mathbf{(1,878,1,1)\to 73}$	$(7,25,2,1)\to 52$	$(8,37,1,1)\to 170$	$(7,82,1,1)\to 374$
19	$(1,746,1,1)\to 21$	$(1,839,1,1)\to 72$	$(11,1,2,5)\to 60$	$(37,5,2,1)\to 196$	$(1,1120,1,1)\to 366$
20	$(1,778,1,1)\to 19$	$\mathbf{(1,1244,1,1)\to 80}$	$(1,451,2,1)\to 44$	$(8,65,1,1)\to 198$	$(25,17,1,1)\to 526$
21	$(1,677,1,1)\to 20$	$(256,1,1,1)\to 80$	$(32,11,1,1)\to 52$	$(125,1,2,1)\to 208$	$(7,115,1,1)\to 446$
22	$(1,788,1,1)\to 24$	$\mathbf{(121,4,1,1)\to 80}$	$(13,19,2,1)\to 64$	$(13,19,2,1)\to 178$	$(16,35,1,1)\to 484$
23	$(1,613,1,1)\to 22$	$(1,1084,1,1)\to 92$	$(208,1,1,1)\to 56$	$(11,35,2,1)\to 214$	$(7,92,1,1)\to 408$
24	$(1,653,1,1)\to 23$	$(1,751,1,1)\to 82$	$(1,11,1,16)\to 54$	$(5,77,2,1)\to 228$	$(5,136,1,1)\to 464$
25	$(1,1460,1,1)\to 22$	$(4,167,1,1)\to 87$	$(5,49,2,1)\to 56$	$(1,31,5,1)\to 222$	$(20,17,1,1)\to 552$
26	$(8,53,1,1)\to 24$	$(1,1436,1,1)\to 92$	$(52,7,1,1)\to 56$	$(19,7,1,4)\to 180$	$(1,79,4,1)\to 462$
27	$(1,1397,1,1)\to 22$	$(4,151,1,1)\to 100$	$(232,1,1,1)\to 56$	$(7,47,2,1)\to 198$	$(7,47,2,1)\to 472$
28	$(1,1730,1,1)\to 20$	$(4,191,1,1)\to 99$	$(7,41,2,1)\to 62$	$(13,68,1,1)\to 212$	$(7,41,2,1)\to 402$
29	$(1,757,1,1)\to 25$	$(8,7,1,5)\to 104$	$(17,19,2,1)\to 62$	$(19,44,1,1)\to 202$	$(8,79,1,1)\to 604$
30	$(1,1114,1,1)\to 25$	$\mathbf{(1,1375,1,1)\to 99}$	$(31,16,1,1)\to 56$	$(1,1,5,7)\to 248$	$(25,34,1,1)\to 475$
31	$(1,1285,1,1)\to 21$	$(1,2159,1,1)\to 102$	$(5,176,1,1)\to 60$	$(11,7,4,1)\to 216$	$(5,61,2,1)\to 522$
32	$(1,1226,1,1)\to 25$	$\mathbf{(1,1039,1,1)\to 112}$	$(23,44,1,1)\to 54$	$(43,22,1,1)\to 215$	$(1,1264,1,1)\to 490$
33	$(1,1108,1,1)\to 31$	$(1,103,1,5)\to 111$	$(40,11,1,1)\to 80$	$(32,17,1,1)\to 256$	$(1,43,5,1)\to 524$
34	$(1,877,1,1)\to 26$	$\mathbf{(1,1678,1,1)\to 113}$	$(4,253,1,1)\to 54$	$(5,67,2,1)\to 246$	$(1,47,5,1)\to 440$
35	$(1,1465,1,1)\to 24$	$\mathbf{(1,1916,1,1)\to 122}$	$(119,5,1,1)\to 72$	$(25,31,1,1)\to 242$	$(28,1,1,5)\to 608$
36	$(1,1192,1,1)\to 24$	$\mathbf{(4,199,1,1)\to 130}$	$(7,53,2,1)\to 72$	$(16,37,1,1)\to 274$	$(16,47,1,1)\to 444$
37	$(1,1268,1,1)\to 28$	$(4,239,1,1)\to 123$	$(7,59,2,1)\to 62$	$(37,5,1,4)\to 222$	$(4,179,1,1)\to 408$
38	$(1,997,1,1)\to 26$	$\mathbf{(1,1231,1,1)\to 131}$	$(1,77,2,5)\to 48$	$(1,185,4,1)\to 228$	$(1,2212,1,1)\to 362$
39	$(4,157,1,1)\to 28$	$(1,1511,1,1)\to 128$	$(23,1,2,5)\to 66$	$(7,95,2,1)\to 268$	$(4,163,1,1)\to 454$
40	$(1,1514,1,1)\to 29$	$\mathbf{(1,1756,1,1)\to 142}$	$(275,2,1,1)\to 54$	$(1,68,5,1)\to 260$	$(1,68,5,1)\to 502$
41	$(1,1384,1,1)\to 24$	$(1,3020,1,1)\to 130$	$(88,7,1,1)\to 56$	$(128,5,1,1)\to 240$	$(145,4,1,1)\to 488$
42	$(1,109,1,5)\to 27$	$\mathbf{(1,1279,1,1)\to 132}$	$(11,41,2,1)\to 64$	$(25,1,1,7)\to 260$	$(13,115,1,1)\to 436$
43	$(1,1117,1,1)\to 32$	$(4,391,1,1)\to 132$	$(1,59,1,7)\to 55$	$(11,35,1,4)\to 252$	$(25,17,2,1)\to 624$
44	$(1,1492,1,1)\to 35$	$\mathbf{(1,1966,1,1)\to 136}$	$(179,4,1,1)\to 54$	$(7,67,2,1)\to 270$	$(19,13,1,4)\to 466$
45	$(1,1706,1,1)\to 25$	$\mathbf{(1,1399,1,1)\to 145}$	$(17,29,2,1)\to 68$	$(161,4,1,1)\to 264$	$(32,35,1,1)\to 604$
46	$(1,1642,1,1)\to 27$	$(1,2455,1,1)\to 139$	$(47,16,1,1)\to 54$	$(1,74,5,1)\to 284$	$(61,17,1,1)\to 442$
47	$(1,1576,1,1)\to 30$	$(1,3598,1,1)\to 139$	$(47,11,2,1)\to 60$	$(55,7,2,1)\to 296$	$(7,115,2,1)\to 462$
48	$(1,1213,1,1)\to 33$	$(1,3484,1,1)\to 144$	$(1,1588,1,1)\to 51$	$(5,77,1,4)\to 259$	$(31,17,2,1)\to 402$
49	$(4,197,1,1)\to 36$	$(4,311,1,1)\to 159$	$(29,1,2,5)\to 72$	$(5,97,2,1)\to 284$	$(5,316,1,1)\to 584$
50	$(1,2285,1,1)\to 28$	$(1,2126,1,1)\to 154$	$(29,19,2,1)\to 74$	$(1,2992,1,1)\to 258$	$(7,236,1,1)\to 514$

Table A.3
Table for $\max\{\#X(n_0, n_{0^+}, n_{\mathrm{ns}}, n_{\mathrm{ns}^+})(\mathbb{F}_q)\}$ with $q = 5^k$ and $n_0 n_{0^+} n_{\mathrm{ns}}^2 n_{\mathrm{ns}^+}^2 \leqslant 10000$.

g	$\mathbb{F}_5$	$\mathbb{F}_{5^2}$	$\mathbb{F}_{5^3}$	$\mathbb{F}_{5^4}$	$\mathbb{F}_{5^5}$
1	$(1,7,1,4)\to 10$	$(1,1,1,21)\to 36$	$(1,132,1,1)\to 148$	$(1,1,1,11)\to 675$	$(1,13,1,4)\to 3227$
2	$(1,67,1,1)\to 12$	$(1,51,1,4)\to 46$	$(1,14,3,1)\to 170$	$(1,67,1,1)\to 724$	$(1,167,1,1)\to 3328$
3	$(4,19,1,1)\to 15$	$(1,19,1,12)\to 56$	$(1,28,3,1)\to 192$	$(1,29,2,1)\to 738$	$(13,1,1,4)\to 3404$
4	$(1,172,1,1)\to 17$	$(4,47,1,1)\to 66$	$(4,33,1,1)\to 174$	$(61,1,1,1)\to 758$	$(1,334,1,1)\to 3530$
5	$(1,278,1,1)\to 16$	$\mathbf{(1,572,1,1)\to 71}$	$(1,1,3,8)\to 170$	$(19,1,1,3)\to 817$	$(1,572,1,1)\to 3631$
6	$(1,163,1,1)\to 19$	$(8,13,1,1)\to 74$	$(3,53,1,1)\to 178$	$(9,13,1,1)\to 902$	$(12,7,1,1)\to 3612$
7	$(1,268,1,1)\to 21$	$(16,9,1,1)\to 84$	$(4,7,3,1)\to 240$	$(1,232,1,1)\to 854$	$(7,33,1,1)\to 3644$
8	$(1,403,1,1)\to 21$	$(1,27,4,1)\to 88$	$(76,1,1,1)\to 174$	$(9,26,1,1)\to 885$	$(1,46,3,1)\to 3684$
9	$(4,43,1,1)\to 24$	$(1,622,1,1)\to 90$	$(93,1,1,1)\to 200$	$(19,9,1,1)\to 898$	$(87,1,1,1)\to 3768$
10	$(1,422,1,1)\to 23$	$(1,668,1,1)\to 108$	$(1,113,2,1)\to 166$	$(4,41,1,1)\to 942$	$\mathbf{(1,668,1,1)\to 4092}$
11	$(1,331,1,1)\to 24$	$(1,503,1,1)\to 109$	$(112,1,1,1)\to 204$	$(39,4,1,1)\to 888$	$(13,23,1,1)\to 3912$
12	$(1,203,1,3)\to 23$	$\mathbf{(16,13,1,1)\to 122}$	$(1,11,3,4)\to 204$	$(1,148,1,3)\to 839$	$(1,868,1,1)\to 3786$
13	$(1,379,1,1)\to 26$	$\mathbf{(4,143,1,1)\to 126}$	$(129,1,1,1)\to 200$	$(9,13,2,1)\to 936$	$(29,9,1,1)\to 3768$
14	$(1,988,1,1)\to 21$	$(1,1007,1,1)\to 117$	$(3,41,2,1)\to 194$	$(19,4,1,3)\to 1000$	$(9,46,1,1)\to 3848$
15	$(4,67,1,1)\to 30$	$(1,719,1,1)\to 127$	$(93,2,1,1)\to 204$	$(21,11,1,1)\to 908$	$(21,11,1,1)\to 4044$
16	$(1,662,1,1)\to 28$	$(1,647,1,1)\to 136$	$(23,3,1,4)\to 180$	$(8,1,1,7)\to 974$	$(68,3,1,1)\to 3852$
17	$(8,11,1,3)\to 28$	$(196,1,1,1)\to 142$	$(8,7,3,1)\to 288$	$(171,1,1,1)\to 1060$	$(1,92,3,1)\to 4186$
18	$(1,499,1,1)\to 31$	$(1,271,1,3)\to 146$	$(9,11,1,4)\to 204$	$(9,52,1,1)\to 1082$	$(13,46,1,1)\to 3858$
19	$(1,652,1,1)\to 33$	$(1,1006,1,1)\to 154$	$(1,112,3,1)\to 240$	$(27,13,1,1)\to 1026$	$(87,1,2,1)\to 4084$
20	$(1,547,1,1)\to 33$	$(1,1052,1,1)\to 164$	$(11,43,1,1)\to 186$	$(1,87,4,1)\to 1096$	$(1,724,1,1)\to 3972$
21	$(3,172,1,1)\to 34$	$(1,743,1,1)\to 152$	$(7,8,3,1)\to 244$	$(1,232,1,3)\to 966$	$(247,1,1,1)\to 3804$
22	$(1,844,1,1)\to 38$	$(121,4,1,1)\to 164$	$(188,1,1,1)\to 246$	$(4,29,1,3)\to 996$	$(1,1242,1,1)\to 4048$
23	$(1,921,1,1)\to 30$	$\mathbf{(1,887,1,1)\to 180}$	$(1,17,8,1)\to 244$	$(1,772,1,1)\to 1096$	$(17,36,1,1)\to 3928$
24	$(1,227,1,3)\to 29$	$\mathbf{(1,412,1,3)\to 188}$	$(1,1989,1,1)\to 204$	$(7,23,1,3)\to 942$	$(1,3,4,7)\to 3764$
25	$(4,171,1,1)\to 30$	$\mathbf{(4,167,1,1)\to 204}$	$(1,11,9,1)\to 210$	$(1,1804,1,1)\to 952$	$(4,167,1,1)\to 4332$
26	$(1,739,1,1)\to 38$	$(1,1294,1,1)\to 188$	$(163,1,2,1)\to 190$	$(1,916,1,1)\to 1114$	$(3,208,1,1)\to 3934$
27	$(3,163,1,1)\to 36$	$\mathbf{(1,1509,1,1)\to 191}$	$(129,1,2,1)\to 196$	$(3,364,1,1)\to 1056$	$(9,92,1,1)\to 4186$
28	$(1,787,1,1)\to 35$	$\mathbf{(1,1336,1,1)\to 200}$	$(7,41,2,1)\to 218$	$(16,29,1,1)\to 1218$	$(9,82,1,1)\to 4060$
29	$(1,1094,1,1)\to 37$	$\mathbf{(1,2004,1,1)\to 200}$	$(93,4,1,1)\to 248$	$(3,232,1,1)\to 1288$	$(9,29,2,1)\to 4202$
30	$(4,139,1,1)\to 39$	$(3,2,1,13)\to 191$	$(1,297,1,4)\to 210$	$(19,17,2,1)\to 1032$	$(367,1,1,1)\to 3888$
31	$(1,1132,1,1)\to 37$	$\mathbf{(1,1532,1,1)\to 228}$	$(1,1,11,4)\to 228$	$(21,11,2,1)\to 1268$	$(204,1,1,1)\to 4332$
32	$(1,1227,1,1)\to 35$	$\mathbf{(1,542,1,3)\to 213}$	$(1,97,4,1)\to 208$	$(3,193,1,1)\to 1150$	$(1,32,1,7)\to 3886$
33	$(3,268,1,1)\to 42$	$\mathbf{(1,1319,1,1)\to 225}$	$(11,14,3,1)\to 218$	$(9,67,1,1)\to 1016$	$(1,184,3,1)\to 4242$
34	$(1,1228,1,1)\to 41$	$\mathbf{(1,1223,1,1)\to 241}$	$(7,1,2,9)\to 190$	$(16,1,1,7)\to 1260$	$(4,23,3,1)\to 4686$
35	$(1,1304,1,1)\to 39$	$\mathbf{(1,1916,1,1)\to 242}$	$(1,194,3,1)\to 230$	$(117,4,1,1)\to 1204$	$(13,92,1,1)\to 4604$
36	$(1,428,1,3)\to 45$	$\mathbf{(1,2327,1,1)\to 236}$	$(1,1908,1,1)\to 218$	$(16,37,1,1)\to 1202$	$(1,1557,1,1)\to 4110$
37	$(1,1324,1,1)\to 46$	$\mathbf{(4,79,1,3)\to 243}$	$(7,59,2,1)\to 218$	$(36,13,1,1)\to 1296$	$(151,4,1,1)\to 4284$
38	$(1,1956,1,1)\to 37$	$(1,2177,1,1)\to 226$	$(9,89,1,1)\to 252$	$(3,229,1,1)\to 1268$	$(1,836,1,3)\to 4026$
39	$(1,1051,1,1)\to 48$	$\mathbf{(1,1774,1,1)\to 260}$	$(16,7,3,1)\to 336$	$(3,29,4,1)\to 1328$	$(13,23,1,3)\to 4012$
40	$(1,1641,1,1)\to 39$	$\mathbf{(1,1559,1,1)\to 264}$	$(163,4,1,1)\to 222$	$(12,41,1,1)\to 1326$	$(12,41,1,1)\to 3966$
41	$(1,1963,1,1)\to 34$	$\mathbf{(3,83,1,4)\to 256}$	$(56,1,3,1)\to 288$	$(17,91,1,1)\to 1168$	$(1,1281,2,1)\to 4074$
42	$(12,43,1,1)\to 48$	$\mathbf{(1,2012,1,1)\to 296}$	$(3,221,2,1)\to 274$	$(1,2316,1,1)\to 1182$	$(1,418,3,1)\to 4128$
43	$(1,1516,1,1)\to 50$	$\mathbf{(3,623,1,1)\to 266}$	$(1,224,3,1)\to 248$	$(1,2088,1,1)\to 1400$	$(1,1556,1,1)\to 4650$
44	$(1,431,1,3)\to 37$	$\mathbf{(1,1487,1,1)\to 289}$	$(16,77,1,1)\to 254$	$(8,29,1,3)\to 1174$	$(8,29,1,3)\to 4166$
45	$(1,3014,1,1)\to 36$	$\mathbf{(1,1427,1,1)\to 275}$	$(3,167,2,1)\to 266$	$(17,29,2,1)\to 1224$	$(63,11,1,1)\to 4564$
46	$(1,76,1,7)\to 40$	$\mathbf{(4,263,1,1)\to 306}$	$(27,44,1,1)\to 244$	$(9,1,1,11)\to 1438$	$(1,7,13,1)\to 4514$
47	$(1,1766,1,1)\to 43$	$\mathbf{(3,383,1,1)\to 298}$	$(81,11,1,1)\to 282$	$(7,99,2,1)\to 1196$	$(9,107,1,1)\to 4414$
48	$(4,211,1,1)\to 57$	$\mathbf{(1,796,1,3)\to 302}$	$(8,97,1,1)\to 222$	$(4,193,1,1)\to 1466$	$(3,89,1,4)\to 4058$
49	$(1,1814,1,1)\to 45$	$\mathbf{(4,311,1,1)\to 315}$	$(36,17,1,1)\to 294$	$(4,351,1,1)\to 1200$	$(27,46,1,1)\to 4718$
50	$(1,1688,1,1)\to 46$	$\mathbf{(1,2396,1,1)\to 306}$	$(9,136,1,1)\to 226$	$(67,4,1,3)\to 1168$	$(3,524,1,1)\to 4324$

Table A.4
Table for $\max\{\#X(n_0, n_{0^+}, n_{\mathrm{ns}}, n_{\mathrm{ns}^+})(\mathbb{F}_q)\}$ with $q = 7^k$ and $n_0 n_{0^+} n_{\mathrm{ns}}^2 n_{\mathrm{ns}^+}^2 \leqslant 10000$.

g	$\mathbb{F}_7$	$\mathbb{F}_{7^2}$	$\mathbb{F}_{7^3}$	$\mathbb{F}_{7^4}$	$\mathbb{F}_{7^5}$
1	$(1,1,1,15)\to 13$	$(1,1,1,11)\to 64$	$(1,76,1,1)\to 380$	$(1,1,1,24)\to 2496$	$(1,4,1,5)\to 17050$
2	$(8,1,1,3)\to 16$	$(1,1,1,16)\to 78$	$(1,33,2,1)\to 412$	$(1,1,4,3)\to 2590$	$(1,8,1,5)\to 17292$
3	$(1,113,1,1)\to 18$	$(1,124,1,3)\to 92$	$(1,71,2,1)\to 446$	$(1,29,2,1)\to 2684$	$(1,290,1,1)\to 17534$
4	$(1,137,1,1)\to 21$	$(20,3,1,1)\to 102$	$(3,55,1,1)\to 440$	$(16,1,1,3)\to 2778$	$(1,22,3,1)\to 17770$
5	$(1,4,1,15)\to 24$	$(52,1,1,1)\to 112$	$(8,11,1,1)\to 440$	$(29,1,2,1)\to 2808$	$(11,9,1,1)\to 18012$
6	$(1,73,1,3)\to 26$	$(1,359,1,1)\to 121$	$(1,33,4,1)\to 480$	$(3,68,1,1)\to 2774$	$(4,3,1,5)\to 17795$
7	$(1,257,1,1)\to 26$	$(1,1,16,1)\to 148$	$(12,11,1,1)\to 474$	$(68,1,1,1)\to 2844$	$(8,1,1,5)\to 18496$
8	$(1,356,1,1)\to 24$	$(1,431,1,1)\to 138$	$(1,4,9,1)\to 508$	$(1,304,1,1)\to 2831$	$(11,20,1,1)\to 18496$
9	$(1,97,1,3)\to 29$	$(1,151,1,3)\to 167$	$(3,76,1,1)\to 528$	$(8,19,1,1)\to 2904$	$\mathbf{(99,1,1,1)\to 18968}$
10	$(1,146,1,3)\to 26$	$(27,1,1,4)\to 153$	$(16,11,1,1)\to 536$	$(19,1,2,3)\to 2976$	$(19,11,1,1)\to 18143$
11	$(1,353,1,1)\to 33$	$\mathbf{(1,764,1,1)\to 176}$	$(3,55,2,1)\to 556$	$(117,1,1,1)\to 3052$	$(17,4,1,3)\to 18724$
12	$(1,452,1,1)\to 36$	$\mathbf{(1,718,1,1)\to 171}$	$(9,38,1,1)\to 548$	$(1,500,1,1)\to 2893$	$(1,43,4,1)\to 17968$
13	$(4,1,1,15)\to 36$	$\mathbf{(1,599,1,1)\to 184}$	$(1,279,2,1)\to 504$	$(9,13,2,1)\to 3048$	$(19,18,1,1)\to 18368$
14	$(1,194,1,3)\to 31$	$\mathbf{(3,43,2,1)\to 194}$	$(3,220,1,1)\to 510$	$(83,1,2,1)\to 3002$	$(1,59,4,1)\to 18520$
15	$(1,548,1,1)\to 40$	$\mathbf{(1,956,1,1)\to 214}$	$(40,1,1,3)\to 584$	$(4,67,1,1)\to 3104$	$(55,4,1,1)\to 19216$
16	$(12,17,1,1)\to 36$	$(81,4,1,1)\to 210$	$(1,796,1,1)\to 526$	$(12,17,1,1)\to 3090$	$(4,11,3,1)\to 18732$
17	$(1,706,1,1)\to 35$	$(1,92,1,5)\to 216$	$(1,9,1,20)\to 532$	$(5,67,1,1)\to 3228$	$(185,1,1,1)\to 18804$
18	$(1,785,1,1)\to 33$	$\mathbf{(1,179,1,4)\to 224}$	$(12,19,1,1)\to 584$	$(16,19,1,1)\to 3118$	$(5,116,1,1)\to 18888$
19	$(1,593,1,1)\to 39$	$(3,191,1,1)\to 232$	$(4,1,9,1)\to 612$	$(27,13,1,1)\to 3267$	$(1,19,1,15)\to 18613$
20	$(1,1394,1,1)\to 33$	$(1,1052,1,1)\to 242$	$(1,34,5,1)\to 478$	$(1,724,1,1)\to 3201$	$(83,4,1,1)\to 18438$
21	$(1,193,1,3)\to 41$	$(3,284,1,1)\to 252$	$(24,11,1,1)\to 632$	$(184,1,1,1)\to 2968$	$(207,1,1,1)\to 19568$
22	$(1,1356,1,1)\to 37$	$(100,3,1,1)\to 246$	$(188,1,1,1)\to 594$	$(4,89,1,1)\to 3174$	$(4,145,1,1)\to 18648$
23	$(1,617,1,1)\to 45$	$(1,911,1,1)\to 264$	$(9,110,1,1)\to 566$	$(9,53,1,1)\to 3308$	$(1,2204,1,1)\to 18811$
24	$(1,292,1,3)\to 44$	$(1,412,1,3)\to 272$	$(1,71,4,1)\to 540$	$(1,307,2,1)\to 3089$	$(1,808,1,1)\to 19211$
25	$(1,16,1,15)\to 36$	$(1,1751,1,1)\to 284$	$(27,1,1,5)\to 660$	$(117,1,2,1)\to 3408$	$(4,101,1,1)\to 19362$
26	$(1,932,1,1)\to 48$	$(1,1436,1,1)\to 312$	$(17,44,1,1)\to 566$	$(1,5,2,11)\to 3165$	$(185,2,1,1)\to 19586$
27	$(8,1,1,15)\to 48$	$(3,23,1,5)\to 288$	$(9,76,1,1)\to 824$	$(232,1,1,1)\to 3340$	$(8,1,1,15)\to 19488$
28	$(4,113,1,1)\to 54$	$(4,191,1,1)\to 330$	$(27,19,1,1)\to 558$	$(16,29,1,1)\to 3498$	$(1,479,2,1)\to 19743$
29	$(1,53,1,8)\to 36$	$(16,1,5,1)\to 304$	$(1,957,2,1)\to 592$	$(9,29,2,1)\to 3352$	$(99,4,1,1)\to 19936$
30	$(1,929,1,1)\to 43$	$(1,1019,1,1)\to 300$	$(3,244,1,1)\to 582$	$(9,94,1,1)\to 3352$	$(1,1850,1,1)\to 18714$
31	$(1,1096,1,1)\to 46$	$(16,5,3,1)\to 324$	$(12,55,1,1)\to 696$	$(80,1,1,3)\to 3396$	$(297,1,1,1)\to 20352$
32	$(1,386,1,3)\to 47$	$(1,1184,1,1)\to 330$	$(3,440,1,1)\to 510$	$(1,31,4,3)\to 3496$	$(1,2390,1,1)\to 18682$
33	$(1,388,1,3)\to 56$	$(1,1724,1,1)\to 370$	$(1,43,5,1)\to 662$	$(4,201,1,1)\to 3578$	$(88,5,1,1)\to 20168$
34	$(4,137,1,1)\to 60$	$(1,1678,1,1)\to 337$	$(9,55,2,1)\to 606$	$(5,67,2,1)\to 3622$	$(13,76,1,1)\to 19650$
35	$(3,257,1,1)\to 52$	$(1,1916,1,1)\to 364$	$(8,165,1,1)\to 556$	$(117,4,1,1)\to 3412$	$(13,29,2,1)\to 19382$
36	$(1,977,1,1)\to 56$	$(1,604,1,3)\to 392$	$(4,199,1,1)\to 656$	$(11,195,1,1)\to 3352$	$(1,604,1,3)\to 19580$
37	$(1,1097,1,1)\to 54$	$(4,79,1,3)\to 408$	$(9,1,1,20)\to 784$	$(351,1,1,1)\to 3366$	$(151,4,1,1)\to 19336$
38	$(1,1937,1,1)\to 48$	$(1,2155,1,1)\to 352$	$(1,1956,1,1)\to 578$	$(1,2320,1,1)\to 3178$	$(1,2678,1,1)\to 18889$
39	$(1,2033,1,1)\to 51$	$(1,1511,1,1)\to 387$	$(4,163,1,1)\to 704$	$(5,31,2,3)\to 3590$	$(5,284,1,1)\to 19984$
40	$(1,1412,1,1)\to 64$	$(4,23,1,5)\to 402$	$(1,2052,1,1)\to 546$	$(27,13,2,1)\to 3504$	$(1,2064,1,1)\to 19478$
41	$(1,1193,1,1)\to 60$	$(3,359,1,1)\to 412$	$(1,19,9,1)\to 600$	$(31,1,1,8)\to 3474$	$(1,152,1,5)\to 19604$
42	$(1,2852,1,1)\to 54$	$(1,2012,1,1)\to 396$	$(5,244,1,1)\to 544$	$(1,2136,1,1)\to 3446$	$(1,22,3,5)\to 19234$
43	$(1,1217,1,1)\to 57$	$\mathbf{(9,43,2,1)\to 444}$	$(48,11,1,1)\to 872$	$(4,267,1,1)\to 3612$	$(20,29,1,1)\to 20766$
44	$(1,697,1,3)\to 53$	$(1,2759,1,1)\to 402$	$(3,481,1,1)\to 512$	$(8,145,1,1)\to 3598$	$(1,1654,1,1)\to 19418$
45	$(1,1604,1,1)\to 56$	$(1,3071,1,1)\to 410$	$(32,33,1,1)\to 760$	$(4,181,1,1)\to 3992$	$(4,19,1,5)\to 20462$
46	$(1,2788,1,1)\to 52$	$(4,263,1,1)\to 450$	$(47,16,1,1)\to 594$	$(3,277,1,1)\to 3964$	$(1,181,2,3)\to 19392$
47	$(1,164,1,5)\to 56$	$(1,3,26,1)\to 416$	$(1,837,2,1)\to 544$	$(1,2412,1,1)\to 3380$	$(1,925,2,1)\to 19272$
48	$(1,317,1,4)\to 62$	$(1,796,1,3)\to 452$	$(9,220,1,1)\to 746$	$(1,577,2,1)\to 3474$	$(13,116,1,1)\to 20284$
49	$(1,4,1,39)\to 48$	$(12,71,1,1)\to 480$	$(1,1,38,1)\to 644$	$(17,67,1,1)\to 3470$	$(36,1,1,5)\to 20880$
50	$(1,2561,1,1)\to 52$	$\mathbf{(1,2396,1,1)\to 506}$	$(27,55,1,1)\to 622$	$(5,268,1,1)\to 4084$	$(8,101,1,1)\to 21084$

Table A.5
Table for $\max\{\#X(n_0, n_{0^+}, n_{\mathrm{ns}}, n_{\mathrm{ns}^+})(\mathbb{F}_q)\}$ with $q = 11^k$ and $n_0 n_{0^+} n_{\mathrm{ns}}^2 n_{\mathrm{ns}^+}^2 \leqslant 10000$.

g	$\mathbb{F}_{11}$	$\mathbb{F}_{11^2}$	$\mathbb{F}_{11^3}$	$\mathbb{F}_{11^4}$	$\mathbb{F}_{11^5}$
1	(1, 20, 1, 3)→18	(1, 1, 1, 15)→144	(1, 43, 1, 1)→1404	(1, 37, 1, 1)→14875	(1, 5, 1, 12)→161854
2	(1, 133, 1, 1)→21	(1, 167, 1, 1)→166	(16, 3, 1, 1)→1468	(1, 161, 1, 1)→15118	(1, 3, 1, 7)→162656
3	(1, 109, 1, 1)→25	(1, 105, 1, 4)→188	(4, 19, 1, 1)→1488	(1, 27, 1, 4)→15287	(1, 312, 1, 1)→163458
4	(1, 148, 1, 1)→27	(1, 32, 1, 3)→210	(1, 172, 1, 1)→1600	(3, 1, 1, 8)→15466	(3, 13, 2, 1)→164260
5	(1, 181, 1, 1)→32	(1, 1, 2, 15)→232	(19, 3, 2, 1)→1494	(1, 378, 1, 1)→15699	(3, 1, 1, 7)→165062
6	(1, 244, 1, 1)→32	(1, 103, 1, 3)→239	(1, 1, 3, 7)→1622	(12, 7, 1, 1)→15590	(3, 52, 1, 1)→165864
7	(1, 229, 1, 1)→37	(1, 64, 1, 3)→276	(4, 5, 3, 1)→1572	(3, 140, 1, 1)→15636	**(1, 12, 1, 7)→166589**
8	(1, 362, 1, 1)→35	(3, 80, 1, 1)→266	(76, 1, 1, 1)→1740	(1, 532, 1, 1)→15673	(1, 468, 1, 1)→165864
9	(1, 101, 1, 3)→36	(1, 1, 10, 3)→320	**(4, 43, 1, 1)→1812**	(9, 28, 1, 1)→16496	**(8, 39, 1, 1)→167544**
10	(1, 458, 1, 1)→38	(108, 1, 1, 1)→306	(43, 4, 1, 1)→1568	(27, 1, 1, 4)→16308	**(3, 104, 1, 1)→168744**
11	(1, 349, 1, 1)→43	(112, 1, 1, 1)→316	(5, 76, 1, 1)→1600	(3, 64, 1, 1)→16012	(39, 4, 1, 1)→166888
12	(1, 436, 1, 1)→44	**(12, 13, 1, 1)→338**	(1, 137, 2, 1)→1760	(1, 703, 1, 1)→16125	**(12, 13, 1, 1)→170676**
13	(1, 37, 1, 5)→40	(25, 1, 2, 3)→408	(1, 1092, 1, 1)→1642	(1, 756, 1, 1)→17241	(4, 1, 7, 1)→165786
14	(1, 52, 1, 5)→44	(1, 2, 13, 1)→341	(95, 2, 1, 1)→1628	(1, 562, 1, 1)→16181	(1, 329, 2, 1)→165858
15	(4, 61, 1, 1)→48	(153, 1, 1, 1)→380	(91, 3, 1, 1)→1724	(27, 14, 1, 1)→16800	(1, 24, 1, 7)→166581
16	(1, 41, 1, 12)→47	**(9, 1, 1, 7)→414**	(4, 83, 1, 1)→1683	(1, 208, 1, 3)→16050	**(3, 4, 1, 7)→172432**
17	(1, 698, 1, 1)→47	(15, 26, 1, 1)→390	(152, 1, 1, 1)→1880	(1, 634, 1, 1)→16135	(1, 936, 1, 1)→168592
18	(3, 109, 1, 1)→44	(9, 52, 1, 1)→422	(19, 16, 1, 1)→1740	(4, 133, 1, 1)→16751	(4, 73, 1, 1)→167268
19	(1, 794, 1, 1)→47	(64, 1, 1, 3)→540	(217, 1, 1, 1)→1744	(36, 7, 1, 1)→17244	(4, 117, 1, 1)→170676
20	(1, 724, 1, 1)→61	(1, 1244, 1, 1)→438	(43, 12, 1, 1)→1772	(1, 665, 2, 1)→16365	(49, 12, 1, 1)→167696
21	(1, 232, 1, 3)→44	**(256, 1, 1, 1)→464**	(8, 43, 1, 1)→1896	(45, 1, 1, 4)→17048	(3, 196, 1, 1)→172508
22	(4, 29, 1, 3)→54	(16, 25, 1, 1)→462	(92, 3, 1, 1)→1788	(1, 1147, 1, 1)→16431	(1, 267, 1, 4)→167708
23	(1, 661, 1, 1)→62	(1, 2204, 1, 1)→471	(1, 777, 2, 1)→1728	(8, 105, 1, 1)→16672	(156, 1, 1, 1)→172572
24	(1, 1189, 1, 1)→54	**(9, 2, 1, 7)→498**	(1, 4, 3, 7)→1800	(293, 1, 1, 1)→16398	(1, 36, 1, 7)→172432
25	(1, 1047, 1, 1)→52	(32, 13, 1, 1)→544	(20, 19, 1, 1)→1824	(1, 673, 1, 1)→16916	**(24, 13, 1, 1)→180048**
26	(1, 916, 1, 1)→69	(3, 208, 1, 1)→502	(3, 323, 1, 1)→1808	(1, 904, 1, 1)→16278	(3, 208, 1, 1)→170676
27	(4, 109, 1, 1)→66	**(9, 76, 1, 1)→584**	(95, 4, 1, 1)→1800	(1, 2490, 1, 1)→16742	(1, 1143, 1, 1)→168884
28	(1, 269, 1, 3)→64	(4, 191, 1, 1)→546	(4, 43, 1, 3)→1812	(27, 16, 1, 1)→17298	(3, 254, 1, 1)→168264
29	(1, 829, 1, 1)→65	(8, 7, 1, 5)→524	(72, 5, 1, 1)→1784	(9, 140, 1, 1)→17694	(1, 203, 3, 1)→171650
30	(3, 244, 1, 1)→64	(1, 1019, 1, 1)→515	(5, 87, 2, 1)→1720	(1, 1512, 1, 1)→17203	(1, 89, 4, 1)→168420
31	(1, 104, 1, 5)→54	(1, 2159, 1, 1)→574	(5, 7, 1, 8)→1864	(27, 28, 1, 1)→19164	(3, 4, 7, 1)→174416
32	(1, 293, 1, 3)→51	(125, 1, 1, 3)→574	(1, 1, 25, 1)→1838	(27, 5, 1, 4)→16766	(3, 8, 1, 7)→172546
33	(4, 13, 1, 5)→66	(1, 439, 1, 3)→608	(13, 3, 1, 8)→1842	(1, 280, 3, 1)→17420	(1, 1764, 1, 1)→172508
34	(1, 404, 1, 3)→68	(12, 1, 1, 7)→624	(5, 137, 1, 1)→2006	(5, 27, 1, 4)→17466	**(12, 1, 1, 7)→180450**
35	(1, 2356, 1, 1)→56	(1, 1916, 1, 1)→620	(228, 1, 1, 1)→2028	(1, 421, 2, 1)→17478	(13, 92, 1, 1)→170088
36	(12, 37, 1, 1)→60	(1, 2080, 1, 1)→658	(149, 4, 1, 1)→1764	(1, 681, 2, 1)→17001	(8, 73, 1, 1)→172324
37	(1, 1021, 1, 1)→77	(36, 13, 1, 1)→720	(152, 3, 1, 1)→2072	(9, 64, 1, 1)→17784	(8, 3, 1, 7)→174120
38	(3, 229, 1, 1)→70	(3, 520, 1, 1)→642	(13, 140, 1, 1)→1946	(7, 37, 1, 3)→17752	(5, 68, 1, 3)→168964
39	(1, 2172, 1, 1)→66	(40, 13, 1, 1)→708	(183, 1, 2, 1)→1972	(8, 133, 1, 1)→17788	(8, 117, 1, 1)→180048
40	(1, 1396, 1, 1)→84	(16, 65, 1, 1)→714	(1, 783, 2, 1)→1835	(16, 13, 1, 3)→17634	(4, 329, 1, 1)→172542
41	(1, 1448, 1, 1)→65	**(128, 1, 1, 3)→880**	(172, 3, 1, 1)→1938	(72, 7, 1, 1)→18544	(147, 4, 1, 1)→174568
42	(4, 301, 1, 1)→66	(1, 2157, 1, 1)→686	(12, 43, 1, 1)→1986	(1, 2136, 1, 1)→17259	(1, 406, 3, 1)→171972
43	(1, 1129, 1, 1)→59	(400, 1, 1, 1)→732	(8, 129, 1, 1)→2068	(27, 1, 1, 8)→18330	(1, 2088, 1, 1)→170956
44	(1, 148, 1, 5)→78	(1, 1966, 1, 1)→697	(8, 89, 1, 1)→1852	(181, 1, 1, 3)→17758	(196, 3, 1, 1)→169398
45	(4, 181, 1, 1)→90	(9, 4, 5, 1)→800	(184, 3, 1, 1)→1832	(40, 21, 1, 1)→17984	(12, 49, 1, 1)→179250
46	(1, 586, 1, 3)→60	(9, 142, 1, 1)→742	(3, 137, 2, 1)→2080	(4, 61, 1, 3)→17712	(1, 4260, 1, 1)→169720
47	(1, 2245, 1, 1)→65	(3, 416, 1, 1)→804	(13, 1, 2, 7)→1846	(1, 3780, 1, 1)→18179	(3, 416, 1, 1)→173304
48	(1, 1588, 1, 1)→75	(1, 796, 1, 3)→818	(1, 274, 3, 1)→1826	(81, 14, 1, 1)→18816	(3, 89, 1, 4)→173222
49	(1, 500, 1, 3)→73	(4, 311, 1, 1)→840	(37, 21, 2, 1)→1964	(384, 1, 1, 1)→17952	(312, 1, 1, 1)→180336
50	(1, 1684, 1, 1)→85	(1, 2396, 1, 1)→830	(7, 149, 1, 1)→1856	(1, 1684, 1, 1)→17711	(412, 1, 1, 1)→170832

Table A.6
Table for $\max\{\#X(n_0, n_{0^+}, n_{\mathrm{ns}}, n_{\mathrm{ns}^+})(\mathbb{F}_q)\}$ with $q = 13^k$ and $n_0 n_{0^+} n_{\mathrm{ns}}^2 n_{\mathrm{ns}^+}^2 \leqslant 10000$.

g	$\mathbb{F}_{13}$	$\mathbb{F}_{13^2}$	$\mathbb{F}_{13^3}$	$\mathbb{F}_{13^4}$	$\mathbb{F}_{13^5}$
1	$(1,1,1,21)\to 21$	$(1,1,1,11)\to 196$	$(1,4,1,5)\to 2290$	$(1,1,1,15)\to 28899$	$(1,1,1,24)\to 372496$
2	$(1,107,1,1)\to 26$	$(1,4,1,7)\to 222$	$(11,4,1,1)\to 2382$	$(1,165,1,1)\to 29166$	$(1,276,1,1)\to 373698$
3	$(1,43,1,3)\to 29$	$(1,4,1,9)\to 242$	$(1,49,1,3)\to 2408$	$(1,43,1,3)\to 29573$	$(1,37,1,3)\to 374900$
4	$(1,214,1,1)\to 31$	$(7,19,1,1)\to 270$	$(7,1,2,3)\to 2478$	$(1,172,1,1)\to 29840$	$(9,14,1,1)\to 376094$
5	$(1,323,1,1)\to 34$	$(1,23,2,3)\to 291$	$(5,44,1,1)\to 2548$	$(1,4,1,15)\to 29950$	$(32,3,1,1)\to 377296$
6	$(1,67,1,3)\to 41$	$(23,1,1,3)\to 308$	$(1,5,4,3)\to 2478$	$(1,609,1,1)\to 29775$	$(12,7,1,1)\to 376094$
7	$(9,7,2,1)\to 36$	$(9,16,1,1)\to 324$	$(1,5,8,1)\to 2600$	$(1,100,1,3)\to 30426$	$(9,16,1,1)\to 377304$
8	$(1,344,1,1)\to 36$	$\mathbf{(1,4,9,1)\to 364}$	$(55,2,1,1)\to 2670$	$(1,344,1,1)\to 29876$	$(1,552,1,1)\to 375968$
9	$(1,428,1,1)\to 46$	$(40,3,1,1)\to 368$	$(24,5,1,1)\to 2600$	$(4,43,1,1)\to 30719$	$\mathbf{(96,1,1,1)\to 382096}$
10	$(1,347,1,1)\to 45$	$(1,37,2,3)\to 390$	$(19,1,2,3)\to 2574$	$(7,60,1,1)\to 31012$	$\mathbf{(27,7,1,1)\to 382887}$
11	$(1,44,1,5)\to 45$	$(5,74,1,1)\to 392$	$(1,45,4,1)\to 2600$	$(8,33,1,1)\to 30156$	$(37,7,1,1)\to 379002$
12	$(1,172,1,3)\to 50$	$(23,1,2,3)\to 422$	$(11,29,1,1)\to 2646$	$(71,1,2,1)\to 31162$	$(79,1,2,1)\to 378298$
13	$(1,467,1,1)\to 49$	$\mathbf{(9,1,1,8)\to 456}$	$(3,79,1,1)\to 2828$	$(5,82,1,1)\to 30826$	$(1,756,1,1)\to 381309$
14	$(1,443,1,1)\to 56$	$\mathbf{(7,19,1,3)\to 442}$	$(7,59,1,1)\to 2644$	$(1,1410,1,1)\to 30560$	$(1,380,1,3)\to 378758$
15	$(1,716,1,1)\to 50$	$(4,61,1,1)\to 482$	$(55,4,1,1)\to 2984$	$(1,16,5,1)\to 30980$	$\mathbf{(27,14,1,1)\to 384496}$
16	$(4,83,1,1)\to 54$	$(3,97,1,1)\to 488$	$(16,7,1,3)\to 2910$	$(1,69,4,1)\to 31380$	$(11,27,1,1)\to 380118$
17	$(1,694,1,1)\to 52$	$\mathbf{(7,3,1,8)\to 500}$	$(73,1,1,3)\to 2608$	$(71,4,1,1)\to 30956$	$(8,69,1,1)\to 381044$
18	$(1,1292,1,1)\to 57$	$(1,271,1,3)\to 524$	$(3,158,1,1)\to 3030$	$(71,1,1,3)\to 31154$	$(1,561,2,1)\to 380465$
19	$(1,19,1,15)\to 52$	$\mathbf{(4,1,9,1)\to 582}$	$(64,5,1,1)\to 2984$	$(132,1,1,1)\to 31548$	$(36,7,1,1)\to 384492$
20	$(1,1041,1,1)\to 50$	$(1,61,4,1)\to 516$	$(29,4,1,3)\to 2614$	$(9,58,1,1)\to 31153$	$(79,1,1,3)\to 383320$
21	$(1,268,1,3)\to 71$	$(45,7,1,1)\to 548$	$(56,1,1,3)\to 2936$	$(8,43,1,1)\to 31580$	$(45,1,1,4)\to 386432$
22	$(4,107,1,1)\to 69$	$\mathbf{(12,25,1,1)\to 594}$	$(7,16,1,3)\to 2922$	$(28,15,1,1)\to 32754$	$(3,385,1,1)\to 384556$
23	$(1,1115,1,1)\to 53$	$\mathbf{(3,476,1,1)\to 594}$	$(1,1422,1,1)\to 2898$	$(1,617,1,1)\to 31089$	$(97,4,1,1)\to 382266$
24	$(1,683,1,1)\to 70$	$(4,183,1,1)\to 626$	$(1,292,1,3)\to 2762$	$(1,71,4,1)\to 31694$	$(1,407,1,3)\to 381949$
25	$(4,11,1,5)\to 60$	$\mathbf{(180,1,1,1)\to 672}$	$(1,158,3,1)\to 2810$	$(1,1827,1,1)\to 31694$	$(4,131,1,1)\to 382905$
26	$(1,326,1,3)\to 61$	$(1,343,2,1)\to 628$	$(1,505,2,1)\to 2824$	$(1,5,2,11)\to 31763$	$(8,53,1,1)\to 382246$
27	$(1,283,1,3)\to 53$	$(1,2,17,1)\to 638$	$(113,1,1,3)\to 2942$	$(71,2,1,3)\to 32030$	$(17,11,1,3)\to 382800$
28	$(4,43,1,3)\to 75$	$(1,1151,1,1)\to 670$	$(4,1,1,21)\to 2898$	$(4,43,1,3)\to 32979$	$(3,227,1,1)\to 381918$
29	$(1,1401,1,1)\to 59$	$(289,2,1,1)\to 682$	$(3,5,8,1)\to 3368$	$(16,1,5,1)\to 32776$	$(17,19,2,1)\to 384860$
30	$(1,344,1,3)\to 64$	$\mathbf{(8,61,1,1)\to 730}$	$(1,2162,1,1)\to 2697$	$(1,344,1,3)\to 32088$	$(79,2,1,3)\to 385836$
31	$(3,263,1,1)\to 58$	$\mathbf{(81,7,1,1)\to 744}$	$(220,1,1,1)\to 3372$	$(3,23,4,1)\to 32168$	$\mathbf{(27,28,1,1)\to 398892}$
32	$(3,332,1,1)\to 72$	$(1,542,1,3)\to 728$	$(1,1264,1,1)\to 2809$	$(5,172,1,1)\to 32060$	$(47,21,1,1)\to 381924$
33	$(1,2086,1,1)\to 61$	$(1,1319,1,1)\to 744$	$(4,201,1,1)\to 3308$	$(5,43,1,3)\to 31964$	$(288,1,1,1)\to 391712$
34	$(1,2060,1,1)\to 67$	$\mathbf{(9,100,1,1)\to 798}$	$(139,4,1,1)\to 2896$	$(284,1,1,1)\to 33606$	$(11,27,2,1)\to 384738$
35	$(1,947,1,1)\to 82$	$(28,19,1,1)\to 796$	$(355,1,1,1)\to 3036$	$(71,8,1,1)\to 32916$	$(37,28,1,1)\to 388916$
36	$(1,1388,1,1)\to 86$	$(1,604,1,3)\to 758$	$(19,58,1,1)\to 2755$	$(1,159,4,1)\to 32482$	$(7,53,2,1)\to 386202$
37	$(1,1366,1,1)\to 76$	$(4,239,1,1)\to 792$	$(4,49,1,3)\to 3204$	$(1,1,2,27)\to 32331$	$(1,1,34,1)\to 384712$
38	$(1,263,1,4)\to 71$	$(16,57,1,1)\to 854$	$(27,2,1,5)\to 2770$	$(3,203,2,1)\to 32838$	$(316,1,1,1)\to 388882$
39	$(1,1676,1,1)\to 62$	$(21,1,1,8)\to 812$	$(3,316,1,1)\to 3736$	$(21,29,1,1)\to 32324$	$(395,1,1,1)\to 385084$
40	$(4,323,1,1)\to 78$	$(1,2471,1,1)\to 844$	$(3,580,1,1)\to 3000$	$(4,265,1,1)\to 32952$	$(79,1,2,3)\to 388218$
41	$(1,1187,1,1)\to 83$	$(441,1,1,1)\to 856$	$(128,5,1,1)\to 3368$	$(88,7,1,1)\to 33344$	$(160,3,1,1)\to 386912$
42	$(1,1163,1,1)\to 81$	$(1,2012,1,1)\to 836$	$(1,1407,2,1)\to 2808$	$(12,43,1,1)\to 32882$	$(1,2196,1,1)\to 384018$
43	$(1,1283,1,1)\to 84$	$(27,1,1,8)\to 933$	$(112,1,1,3)\to 3660$	$(84,5,1,1)\to 33252$	$(289,1,2,1)\to 391428$
44	$(3,428,1,1)\to 92$	$(1,1487,1,1)\to 863$	$(8,145,1,1)\to 2970$	$(7,240,1,1)\to 31474$	$(59,4,1,3)\to 388810$
45	$(1,1367,1,1)\to 74$	$(1,12,11,1)\to 936$	$(1,45,8,1)\to 3220$	$(56,15,1,1)\to 33280$	$(141,4,1,1)\to 392568$
46	$(4,67,1,3)\to 102$	$(4,55,3,1)\to 894$	$(9,134,1,1)\to 3063$	$(12,77,1,1)\to 32718$	$(1,2323,1,1)\to 388185$
47	$(1,536,1,3)\to 79$	$(3,253,2,1)\to 928$	$(1,28,9,1)\to 3116$	$(213,1,2,1)\to 33516$	$(21,55,1,1)\to 392126$
48	$(1,1772,1,1)\to 110$	$\mathbf{(9,97,1,1)\to 1058}$	$(1,1588,1,1)\to 2864$	$(1,430,3,1)\to 32480$	$(8,97,1,1)\to 385894$
49	$(4,227,1,1)\to 84$	$(225,1,2,1)\to 1040$	$(1,2844,1,1)\to 3472$	$(27,46,1,1)\to 32134$	$(4,227,1,1)\to 388284$
50	$(1,1499,1,1)\to 75$	$(1,2302,1,1)\to 968$	$(103,11,1,1)\to 2786$	$(1,1696,1,1)\to 32230$	$(27,55,1,1)\to 385532$

Table A.7
Table for $\max\{\#X(n_0, n_{0^+}, n_{\mathrm{ns}}, n_{\mathrm{ns}^+})(\mathbb{F}_q)\}$ with $q = 17^k$ and $n_0 n_{0^+} n_{\mathrm{ns}}^2 n_{\mathrm{ns}^+}^2 \leqslant 10000$.

g	$\mathbb{F}_{17}$	$\mathbb{F}_{17^2}$	$\mathbb{F}_{17^3}$	$\mathbb{F}_{17^4}$	$\mathbb{F}_{17^5}$
1	(1, 190, 1, 1)→25	(1, 1, 1, 11)→324	(1, 61, 1, 1)→5054	(1, 3, 1, 8)→84096	(1, 2, 1, 9)→1422141
2	(1, 23, 1, 3)→30	(1, 161, 1, 1)→358	(3, 29, 1, 1)→5166	(1, 88, 1, 1)→84670	(1, 14, 1, 5)→1424424
3	(1, 127, 1, 1)→36	(1, 71, 2, 1)→392	(4, 1, 1, 5)→5256	(3, 70, 1, 1)→85244	(33, 1, 1, 1)→1426584
4	(16, 5, 1, 1)→42	(1, 31, 2, 3)→426	(7, 20, 1, 1)→5350	(12, 5, 1, 1)→85818	(1, 7, 5, 1)→1429090
5	(1, 316, 1, 1)→38	(9, 1, 4, 1)→448	(5, 31, 1, 1)→5390	(3, 40, 1, 1)→85496	(1, 208, 1, 1)→1430904
6	(1, 92, 1, 3)→46	(3, 2, 5, 1)→460	(1, 47, 1, 4)→5372	(1, 24, 1, 5)→86345	(8, 13, 1, 1)→1432818
7	(1, 3, 1, 16)→40	(16, 9, 1, 1)→516	(5, 11, 1, 3)→5572	(1, 365, 1, 1)→86577	(1, 129, 2, 1)→1431052
8	(1, 412, 1, 1)→50	(1, 545, 1, 1)→508	(1, 44, 3, 1)→5482	(1, 412, 1, 1)→86662	(1, 540, 1, 1)→1432069
9	(32, 5, 1, 1)→48	(99, 1, 1, 1)→560	(31, 3, 2, 1)→5602	(24, 5, 1, 1)→86896	**(41, 4, 1, 1)→1438108**
10	(1, 31, 1, 5)→53	(108, 1, 1, 1)→630	(25, 12, 1, 1)→5482	(3, 88, 1, 1)→88046	(1, 416, 1, 1)→1435932
11	(1, 508, 1, 1)→62	(49, 1, 1, 3)→592	(5, 76, 1, 1)→5620	(112, 1, 1, 1)→87148	**(104, 1, 1, 1)→1438748**
12	(1, 184, 1, 3)→56	(1, 1, 4, 7)→630	(1, 169, 2, 1)→5616	(1, 137, 2, 1)→86722	**(16, 13, 1, 1)→1445778**
13	(4, 23, 1, 3)→66	**(144, 1, 1, 1)→696**	(5, 99, 1, 1)→5668	(3, 79, 1, 1)→87166	(143, 1, 1, 1)→1436100
14	(1, 988, 1, 1)→56	(1, 13, 4, 3)→676	(27, 11, 1, 1)→5664	(1, 1030, 1, 1)→86795	(11, 13, 2, 1)→1437974
15	(15, 7, 2, 1)→52	(1, 16, 1, 7)→703	(155, 1, 1, 1)→5632	(1, 792, 1, 1)→87972	**(1, 80, 3, 1)→1445778**
16	(1, 463, 1, 1)→64	(1, 208, 1, 3)→762	(7, 20, 1, 3)→5782	(16, 23, 1, 1)→87522	(1, 1419, 1, 1)→1439212
17	(1, 487, 1, 1)→72	(1, 11, 7, 1)→750	(5, 11, 3, 1)→6100	(37, 12, 1, 1)→88710	(1, 64, 3, 1)→1438724
18	(4, 103, 1, 1)→75	**(1, 271, 1, 3)→746**	(1, 628, 1, 1)→5861	(4, 103, 1, 1)→88715	(1, 1032, 1, 1)→1436450
19	(1, 607, 1, 1)→66	(225, 1, 1, 1)→836	(1, 229, 2, 1)→5708	(48, 5, 1, 1)→89052	(164, 1, 1, 1)→1449636
20	(1, 284, 1, 3)→60	**(8, 13, 1, 3)→862**	(1, 61, 4, 1)→5794	(3, 61, 2, 1)→87914	(143, 2, 1, 1)→1441098
21	(1, 892, 1, 1)→72	**(45, 1, 1, 4)→824**	(5, 41, 2, 1)→5792	(125, 1, 2, 1)→88208	(27, 20, 1, 1)→1446644
22	(1, 23, 1, 9)→70	(4, 215, 1, 1)→864	(1, 220, 3, 1)→5846	(1, 411, 2, 1)→88554	(188, 1, 1, 1)→1442166
23	(1, 974, 1, 1)→74	(1, 36, 5, 1)→816	(5, 44, 1, 3)→5848	(208, 1, 1, 1)→88324	(208, 1, 1, 1)→1454436
24	(4, 127, 1, 1)→93	**(1, 981, 1, 1)→880**	(1, 898, 1, 1)→5851	(3, 115, 2, 1)→87682	(5, 97, 1, 1)→1441184
25	(1, 163, 1, 4)→79	**(49, 1, 2, 3)→990**	(3, 83, 2, 1)→5946	(1, 1460, 1, 1)→90199	(32, 13, 1, 1)→1458896
26	(1, 1351, 1, 1)→63	(1, 343, 2, 1)→884	(1, 507, 2, 1)→6080	(5, 103, 1, 1)→89642	(1, 1203, 1, 1)→1444846
27	(1, 263, 1, 3)→72	(5, 148, 1, 1)→970	(3, 47, 1, 4)→6246	(7, 64, 1, 1)→89420	(33, 13, 1, 1)→1454252
28	(1, 79, 1, 5)→80	(16, 27, 1, 1)→954	(3, 227, 1, 1)→5880	(1, 143, 4, 1)→88598	(4, 47, 1, 3)→1446690
29	(8, 23, 1, 3)→88	**(99, 4, 1, 1)→1000**	(45, 11, 1, 1)→6292	(1, 1626, 1, 1)→88391	(9, 80, 1, 1)→1449606
30	(1, 823, 1, 1)→95	(13, 74, 1, 1)→967	(8, 61, 1, 1)→5942	(9, 61, 1, 1)→92918	(5, 203, 1, 1)→1448331
31	(1, 368, 1, 3)→70	**(4, 455, 1, 1)→1038**	(4, 41, 1, 3)→6018	(1, 2520, 1, 1)→88688	(16, 5, 3, 1)→1461144
32	(1, 1454, 1, 1)→75	(1, 32, 1, 7)→1054	(1, 205, 2, 3)→6220	(1, 2163, 1, 1)→89129	(4, 7, 5, 1)→1444680
33	(1, 124, 1, 5)→82	(25, 1, 1, 8)→1038	(8, 11, 3, 1)→6240	(4, 259, 1, 1)→88796	(13, 1, 8, 1)→1451692
34	(1, 883, 1, 1)→73	**(16, 1, 1, 7)→1260**	(28, 5, 1, 3)→6102	(1, 2060, 1, 1)→92738	(1, 206, 3, 1)→1446024
35	(1, 2332, 1, 1)→87	(304, 1, 1, 1)→1084	(327, 1, 1, 1)→6136	(13, 19, 1, 3)→92680	(3, 1, 16, 1)→1448348
36	(1, 1927, 1, 1)→81	(1, 604, 1, 3)→1064	(31, 13, 2, 1)→6010	(8, 73, 1, 1)→88394	(3, 292, 1, 1)→1449610
37	(1, 1468, 1, 1)→94	(324, 1, 1, 1)→1224	(320, 1, 1, 1)→6552	(19, 56, 1, 1)→89848	(64, 1, 3, 1)→1451520
38	(1, 2360, 1, 1)→72	**(1, 416, 1, 3)→1224**	(1, 77, 2, 5)→6394	(76, 7, 1, 1)→91222	(37, 23, 1, 1)→1443873
39	(1, 526, 1, 3)→79	(369, 1, 1, 1)→1148	(4, 157, 1, 1)→6738	(9, 79, 1, 1)→93212	(328, 1, 1, 1)→1469476
40	(1, 2812, 1, 1)→75	(16, 13, 1, 3)→1434	(1, 183, 4, 1)→5942	(7, 183, 1, 1)→89452	(44, 13, 1, 1)→1463658
41	(1, 1087, 1, 1)→104	(8, 231, 1, 1)→1200	(13, 11, 3, 1)→6332	(72, 7, 1, 1)→92080	(9, 11, 4, 1)→1456004
42	(1, 1646, 1, 1)→101	(12, 43, 1, 1)→1250	(1, 41, 4, 3)→6350	(1, 2136, 1, 1)→90030	(173, 4, 1, 1)→1458362
43	(4, 71, 1, 3)→84	(8, 81, 1, 1)→1308	(523, 1, 1, 1)→6058	(4, 267, 1, 1)→92988	(5, 406, 1, 1)→1454311
44	(1, 568, 1, 3)→80	(1, 2759, 1, 1)→1209	(179, 4, 1, 1)→5876	(89, 12, 1, 1)→89410	(3, 428, 1, 1)→1457298
45	(4, 223, 1, 1)→105	(9, 4, 5, 1)→1392	(5, 396, 1, 1)→6128	(9, 124, 1, 1)→92240	(376, 1, 1, 1)→1451608
46	(1, 28, 1, 11)→82	(3, 139, 2, 1)→1266	(27, 44, 1, 1)→6378	(3, 137, 2, 1)→92478	(108, 5, 1, 1)→1457166
47	(1, 3278, 1, 1)→77	(1, 4991, 1, 1)→1312	(81, 11, 1, 1)→6258	(5, 372, 1, 1)→91346	(31, 5, 3, 1)→1455628
48	(1, 1327, 1, 1)→110	(1, 419, 1, 4)→1326	(5, 47, 1, 4)→6272	(1, 763, 1, 3)→90002	(11, 155, 1, 1)→1453916
49	(1, 1303, 1, 1)→119	(4, 311, 1, 1)→1356	(8, 285, 1, 1)→6364	(1, 3100, 1, 1)→91704	(416, 1, 1, 1)→1476512
50	(1, 2126, 1, 1)→85	(3, 860, 1, 1)→1396	(5, 297, 1, 1)→6572	(3, 151, 2, 1)→92038	(1, 659, 2, 1)→1447175

Table A.8
Table for $\max\{\#X(n_0, n_{0^+}, n_{\mathrm{ns}}, n_{\mathrm{ns}^+})(\mathbb{F}_q)\}$ with $q = 19^k$ and $n_0 n_{0^+} n_{\mathrm{ns}}^2 n_{\mathrm{ns}^+}^2 \leqslant 10000$.

g	$\mathbb{F}_{19}$	$\mathbb{F}_{19^2}$	$\mathbb{F}_{19^3}$	$\mathbb{F}_{19^4}$	$\mathbb{F}_{19^5}$
1	$(1,1,1,24)\to 28$	$(1,1,1,11)\to 400$	$(1,3,1,8)\to 7024$	$(1,11,1,3)\to 131040$	$(1,43,1,1)\to 2478982$
2	$(1,5,1,7)\to 32$	$(1,29,1,3)\to 438$	$(5,12,1,1)\to 7188$	$(1,5,1,7)\to 131758$	$(1,191,1,1)\to 2482286$
3	$(1,149,1,1)\to 38$	$(11,5,1,1)\to 476$	$(9,1,1,4)\to 7352$	$(1,23,1,4)\to 132476$	$(23,2,1,1)\to 2484746$
4	$(1,305,1,1)\to 39$	$(1,319,1,1)\to 504$	$(1,79,2,1)\to 7249$	$(1,260,1,1)\to 133194$	$(1,262,1,1)\to 2487889$
5	$(1,212,1,1)\to 42$	$(11,12,1,1)\to 536$	$(9,1,4,1)\to 7352$	$(1,130,1,3)\to 132984$	$(23,4,1,1)\to 2490510$
6	$(1,269,1,1)\to 43$	$(1,73,1,3)\to 560$	$(29,4,1,1)\to 7420$	$(8,13,1,1)\to 133478$	$(1,103,1,3)\to 2490728$
7	$(1,298,1,1)\to 47$	$(1,671,1,1)\to 585$	$(5,27,1,1)\to 7464$	$(3,35,2,1)\to 133428$	$(4,45,1,1)\to 2490516$
8	$(1,505,1,1)\to 43$	$(1,4,9,1)\to 616$	$(9,35,1,1)\to 7534$	$(7,39,1,1)\to 133678$	$(103,1,1,1)\to 2490892$
9	$(1,404,1,1)\to 49$	$(128,1,1,1)\to 688$	$(21,1,1,4)\to 7676$	$(13,20,1,1)\to 134816$	$(1,11,2,5)\to 2494874$
10	$(1,394,1,1)\to 51$	$(92,1,1,1)\to 702$	$(27,7,1,1)\to 7848$	$(4,65,1,1)\to 135582$	$\mathbf{(92,1,1,1)\to 2499156}$
11	$(1,389,1,1)\to 64$	$(117,1,1,1)\to 724$	$(13,1,1,12)\to 7612$	$(1,13,2,5)\to 134932$	$\mathbf{(17,4,1,3)\to 2501908}$
12	$(1,461,1,1)\to 58$	$(3,1,2,7)\to 750$	$(4,7,1,5)\to 7646$	$(16,13,1,1)\to 135482$	$(17,3,1,4)\to 2500509$
13	$(4,53,1,1)\to 60$	$(1,335,2,1)\to 743$	$(9,1,1,8)\to 7900$	$(3,8,1,5)\to 135354$	$(1,275,2,1)\to 2502798$
14	$(1,509,1,1)\to 65$	$(3,146,1,1)\to 790$	$(59,6,1,1)\to 7987$	$(1,260,1,3)\to 138038$	$(16,21,1,1)\to 2496276$
15	$(1,596,1,1)\to 73$	$(3,49,2,1)\to 816$	$(27,14,1,1)\to 7676$	$(9,31,1,1)\to 136520$	$(153,1,1,1)\to 2503472$
16	$(1,53,1,5)\to 62$	$(1,657,1,1)\to 870$	$(7,75,1,1)\to 7682$	$(4,195,1,1)\to 137010$	$(131,2,1,1)\to 2500451$
17	$(1,218,1,3)\to 60$	$(148,1,1,1)\to 844$	$(65,4,1,1)\to 7836$	$(1,954,1,1)\to 135986$	$(85,1,2,1)\to 2498104$
18	$(3,149,1,1)\to 70$	$(4,73,1,1)\to 854$	$(3,175,1,1)\to 7604$	$(3,260,1,1)\to 137262$	$(5,116,1,1)\to 2495456$
19	$(1,137,1,4)\to 60$	$(1,1,5,12)\to 900$	$(177,1,1,1)\to 7726$	$(52,5,1,1)\to 138036$	$(11,52,1,1)\to 2504088$
20	$(1,778,1,1)\to 71$	$(1,1244,1,1)\to 898$	$(3,7,1,8)\to 8004$	$(8,65,1,1)\to 137706$	$(1,866,1,1)\to 2500405$
21	$(1,229,1,3)\to 74$	$(147,2,1,1)\to 990$	$(45,7,1,1)\to 8408$	$(1,268,1,3)\to 136514$	$(184,1,1,1)\to 2510840$
22	$(1,788,1,1)\to 71$	$(1,1314,1,1)\to 954$	$(1,939,1,1)\to 7865$	$(12,25,1,1)\to 138078$	$(9,68,1,1)\to 2508032$
23	$(3,212,1,1)\to 72$	$\mathbf{(3,1,14,1)\to 988}$	$(1,3,2,13)\to 7788$	$(9,4,1,5)\to 137176$	$(17,36,1,1)\to 2516432$
24	$(1,653,1,1)\to 65$	$(1,29,5,1)\to 990$	$(21,26,1,1)\to 7884$	$(23,1,1,12)\to 136514$	$(1,412,1,3)\to 2513990$
25	$(4,101,1,1)\to 72$	$(4,121,1,1)\to 1035$	$(13,9,1,4)\to 8312$	$(32,13,1,1)\to 140432$	$(68,1,1,3)\to 2521824$
26	$(8,53,1,1)\to 80$	$(1,146,3,1)\to 1042$	$(28,13,1,1)\to 7996$	$(7,156,1,1)\to 137452$	$(8,17,1,3)\to 2511764$
27	$(1,821,1,1)\to 88$	$(1,976,1,1)\to 1116$	$(9,13,1,4)\to 8156$	$(5,187,1,1)\to 138692$	$(25,11,2,1)\to 2515812$
28	$(12,29,1,1)\to 84$	$(1,3036,1,1)\to 1095$	$(236,1,1,1)\to 8190$	$(1,2340,1,1)\to 142106$	$(11,25,2,1)\to 2514876$
29	$(1,106,1,5)\to 82$	$\mathbf{(99,4,1,1)\to 1216}$	$(63,1,1,4)\to 8656$	$(5,52,1,3)\to 142264$	$(1,1537,1,1)\to 2518632$
30	$(1,1341,1,1)\to 76$	$\mathbf{(8,61,1,1)\to 1202}$	$(1,307,1,3)\to 7730$	$(12,31,1,1)\to 137906$	$(9,61,1,1)\to 2506088$
31	$(4,221,1,1)\to 78$	$\mathbf{(9,1,7,1)\to 1260}$	$(27,35,1,1)\to 8862$	$(4,65,1,3)\to 141924$	$(9,17,1,4)\to 2512864$
32	$(1,1527,1,1)\to 81$	$\mathbf{(11,140,1,1)\to 1236}$	$(4,7,5,1)\to 8140$	$(1,2296,1,1)\to 135780$	$(131,4,1,1)\to 2509080$
33	$(1,349,1,3)\to 77$	$(4,219,1,1)\to 1226$	$(7,4,5,1)\to 7928$	$(24,1,1,5)\to 139664$	$(309,1,1,1)\to 2516440$
34	$(1,1109,1,1)\to 82$	$(5,67,2,1)\to 1230$	$(284,1,1,1)\to 7962$	$(9,100,1,1)\to 139794$	$(23,40,1,1)\to 2509530$
35	$(1,2132,1,1)\to 81$	$(49,18,1,1)\to 1256$	$(21,25,1,1)\to 8212$	$(7,198,1,1)\to 139180$	$(1,907,1,1)\to 2508643$
36	$(1,436,1,3)\to 92$	$(9,73,1,1)\to 1490$	$(1,681,2,1)\to 8025$	$(1,1812,1,1)\to 141771$	$(1,553,1,3)\to 2508416$
37	$(4,149,1,1)\to 108$	$\mathbf{(9,1,2,7)\to 1452}$	$(1,1252,1,1)\to 8692$	$(8,195,1,1)\to 141368$	$(4,275,1,1)\to 2524158$
38	$(1,1061,1,1)\to 112$	$(31,25,1,1)\to 1276$	$(1,1185,2,1)\to 7844$	$(9,106,1,1)\to 139805$	$(5,68,1,3)\to 2506686$
39	$(1,1841,1,1)\to 77$	$(1,286,1,5)\to 1312$	$(21,1,1,8)\to 8444$	$(104,5,1,1)\to 141252$	$(123,4,1,1)\to 2525140$
40	$(1,37,1,15)\to 90$	$(4,23,1,5)\to 1386$	$(109,10,1,1)\to 7976$	$(12,65,1,1)\to 143874$	$(44,13,1,1)\to 2522796$
41	$(1,1945,1,1)\to 83$	$(441,1,1,1)\to 1480$	$(315,1,1,1)\to 8752$	$(9,5,1,8)\to 139504$	$(23,52,1,1)\to 2523780$
42	$(1,1229,1,1)\to 103$	$(13,73,1,1)\to 1364$	$(11,41,2,1)\to 8152$	$(25,1,1,7)\to 139658$	$(1,2406,1,1)\to 2514753$
43	$(1,1556,1,1)\to 125$	$(84,5,1,1)\to 1428$	$(405,1,1,1)\to 8448$	$(1,1556,1,1)\to 141021$	$(92,7,1,1)\to 2518236$
44	$(1,2501,1,1)\to 97$	$(3,1001,1,1)\to 1402$	$(49,26,1,1)\to 8486$	$(1,1599,2,1)\to 138385$	$(1,4242,1,1)\to 2515428$
45	$(1,421,1,3)\to 116$	$(1,719,2,1)\to 1458$	$(1,35,1,11)\to 8087$	$(9,124,1,1)\to 141752$	$(161,4,1,1)\to 2531308$
46	$(1,1642,1,1)\to 101$	$(8,1,1,11)\to 1542$	$(1,28,1,11)\to 8832$	$(12,77,1,1)\to 140142$	$(16,105,1,1)\to 2521700$
47	$(1,1576,1,1)\to 89$	$(1,28,9,1)\to 1528$	$(291,2,1,1)\to 7874$	$(15,62,1,1)\to 140160$	$(153,4,1,1)\to 2545480$
48	$(3,89,1,4)\to 92$	$(1,796,1,3)\to 1640$	$(5,378,1,1)\to 8006$	$(1,2538,1,1)\to 138845$	$(1,578,1,3)\to 2517253$
49	$(1,2996,1,1)\to 102$	$(9,49,2,1)\to 1668$	$(175,4,1,1)\to 8636$	$(36,1,1,5)\to 145608$	$(68,9,1,1)\to 2543304$
50	$(1,1844,1,1)\to 113$	$\mathbf{(9,146,1,1)\to 1750}$	$(1,21,5,4)\to 8572$	$(1,2992,1,1)\to 140498$	$(303,2,1,1)\to 2520964$

References

[1] N. Adžaga, V. Arul, L. Beneish, M. Chen, S. Chidambaram, T. Keller, B. Wen, Quadratic Chabauty for Atkin-Lehner Quotients of Modular Curves of Prime Level and Genus 4, 5, 6, 2021.

[2] A.O.L. Atkin, J. Lehner, Hecke operators on $\Gamma_0(m)$, Math. Ann. 185 (1970) 134–160, MR 268123.

[3] Alex J. Best, Jonathan Bober, Andrew R. Booker, Edgar Costa, John E. Cremona, Maarten Derickx, Min Lee, David Lowry-Duda, David Roe, Andrew V. Sutherland, John Voight, in: Jennifer S. Balakrishnan, Noam Elkies, Brendan Hassett, Bjorn Poonen, Andrew V. Sutherland, John Voight (Eds.), Computing Classical Modular Forms, Arithmetic Geometry, Number Theory, and Computation (Cham), Springer International Publishing, 2021, pp. 131–213.

[4] J. Balakrishnan, N. Dogra, J.S. Müller, J. Tuitman, J. Vonk, Explicit Chabauty-Kim for the split Cartan modular curve of level 13, Ann. Math. (2) 189 (3) (2019) 885–944, MR 3961086.

[5] F. Bars, J. González, The automorphism group of the modular curve $X_0^*(N)$ with square-free level, Trans. Am. Math. Soc. 374 (8) (2021) 5783–5803, MR 4293788.

[6] M.H. Baker, E. González-Jiménez, J. González, B. Poonen, Finiteness results for modular curves of genus at least 2, Am. J. Math. 127 (6) (2005) 1325–1387, MR 2183527 (2006i:11065).

[7] A. Brumer, The rank of $J_0(N)$, in: Columbia University Number Theory Seminar (New York, 1992), Astérisque 228 (3) (1995) 41–68, MR 1330927.

[8] I. Chen, The Jacobians of non-split Cartan modular curves, Proc. Lond. Math. Soc. (3) 77 (1) (1998) 1–38, MR 1625491 (99m:11068).

[9] I. Chen, Jacobians of modular curves associated to normalizers of Cartan subgroups of level p^n, C. R. Math. Acad. Sci. Paris 339 (3) (2004) 187–192, MR 2078072.

[10] V. Dose, J. Fernández, J. González, R. Schoof, The automorphism group of the non-split Cartan modular curve of level 11, J. Algebra 417 (2014) 95–102, MR 3244639.

[11] V. Dose, G. Lido, P. Mercuri, Automorphisms of Cartan modular curves of prime and composite level, Algebra Number Theory 16 (6) (2022) 1423–1461, MR 4488580.

[12] V. Dose, P. Mercuri, C. Stirpe, Double covers of Cartan modular curves, J. Number Theory 195 (2019) 96–114, MR 3867436.

[13] V. Dose, On the automorphisms of the nonsplit Cartan modular curves of prime level, Nagoya Math. J. 224 (1) (2016) 74–92, MR 3572750.

[14] F. Diamond, J. Shurman, A First Course in Modular Forms, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005, MR 2112196 (2006f:11045).

[15] B. de Smit, B. Edixhoven, Sur un résultat d'Imin Chen, Math. Res. Lett. 7 (2–3) (2000) 147–153, MR 1764312 (2001j:11043).

[16] Sam Frengley, Congruences of elliptic curves arising from nonsurjective mod n Galois representations, Math. Comput. 92 (339) (2023) 409–450.

[17] G.H. Hardy, E.M. Wright, An Introduction to the Theory of Numbers, sixth ed., Oxford University Press, Oxford, 2008, Revised by D.R. Heath-Brown and J.H. Silverman, with a foreword by Andrew Wiles, MR 2445243.

[18] The LMFDB Collaboration, The L-functions and modular forms database, http://www.lmfdb.org, 2022. (Accessed 1 September 2022), Online.

[19] P. Mercuri, Equations and rational points of the modular curves $X_0^+(p)$, Ramanujan J. 47 (2) (2018) 291–308, MR 3863642.

[20] J.S. Milne, Abelian varieties, in: Arithmetic Geometry, Storrs, Conn., 1984, Springer, New York, 1986, pp. 103–150, MR 861974.

[21] J.S. Milne, Jacobian varieties, in: Arithmetic Geometry, Storrs, Conn., 1984, Springer, New York, 1986, pp. 167–212, MR 861976.

[22] P. Michaud-Rodgers, Quadratic points on non-split Cartan modular curves, Int. J. Number Theory 18 (2) (2022) 245–267, MR 4390660.

[23] P. Mercuri, R. Schoof, Modular forms invariant under non-split Cartan subgroups, Math. Comput. 89 (324) (2020) 1969–1991, MR 4081925.

[24] J.-L. Nicolas, G. Robin, Majorations explicites pour le nombre de diviseurs de n, Can. Math. Bull. 26 (4) (1983) 485–492.

[25] A.P. Ogg, Hyperelliptic modular curves, Bull. Soc. Math. Fr. 102 (1974) 449–462, MR 0364259 (51 #514).

[26] J. Rouse, A.V. Sutherland, D. Zureick-Brown, ℓ-adic images of Galois for elliptic curves over (and an appendix with John Voight), Forum Math. Sigma 10 (2022) e62, MR 4468989.

[27] H. Stichtenoth, Algebraic Function Fields and Codes, second ed., Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin, 2009, MR 2464941.

[28] M.A. Tsfasman, S.G. Vlăduţ, T. Zink, Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound, Math. Nachr. 109 (1982) 21–28, MR 705893.
[29] S.G. Vlèduts, V.G. Drinfel'd, The number of points of an algebraic curve, Funkc. Anal. Prilozh. 17 (1) (1983) 68–69, MR 695100.
[30] G. van der Geer, E. Howe, K. Lauter, C. Ritzenthaler, Tables of curves with many points, http://www.manypoints.org, Snapshot of the website on the 27 August 2022 available at https://web.archive.org/web/20220827113418/https://manypoints.org/.
[31] C.P. Xing, H. Stichtenoth, The genus of maximal function fields over finite fields, Manuscr. Math. 86 (2) (1995) 217–224, MR 1317746.