RADICAL ISOGENIES AND MODULAR CURVES

VALENTINA PRIBANIĆ

Department of Mathematics, University of Zagreb
Bijenička cesta 30, 10000 Zagreb, Croatia

Abstract. This article explores the connection between radical isogenies and modular curves. Radical isogenies are formulas designed for the computation of chains of isogenies of fixed small degree N, introduced by Castryck, Decru, and Vercauteren at Asiacrypt 2020. One significant advantage of radical isogeny formulas over other formulas with a similar purpose is that they eliminate the need to generate a point of order N that generates the kernel of the isogeny. While radical isogeny formulas were originally developed using elliptic curves in Tate normal form, Onuki and Moriya have proposed radical isogeny formulas of degrees 3 and 4 on Montgomery curves and attempted to obtain a simpler form of radical isogenies using enhanced elliptic and modular curves. In this article, we translate the original setup of radical isogenies in Tate normal form into the language of modular curves. Additionally, we solve an open problem introduced by Onuki and Moriya regarding radical isogeny formulas on $X_0(N)$.

Contents

1 Introduction **1**
Paper organization **3**
2 Preliminaries **3**
2.1 Elliptic curves 3
2.2 Isogenies of elliptic curves 4
2.3 Congruence subgroups, modular and enhanced elliptic curves 4
2.4 Semidirect product of groups 6
2.5 Radical isogenies 6
2.5.1 Radical isogenies on Montgomery curves 7
3 Radical isogenies in the language of modular curves **8**
3.1 "Shrinking" the field of definition 9
4 Extending to $X_0(N)$ **14**
References **18**

1. Introduction

Post-quantum cryptography (PQC) is an area of cryptography focused on developing cryptosystems that can resist attacks from both classical and quantum computers. These systems rely on hard mathematical problems that differ from the integer factorization problem or (elliptic-curve) discrete logarithm problem, which are the basis of most current cryptographic

E-mail address: valentina.pribanic@gmail.com.

2020 *Mathematics Subject Classification.* Primary 94A60, 11T71, Secondary 11G05.

Key words and phrases. elliptic curves, isogenies, radical isogenies, modular curves, post-quantum cryptography.

algorithms. PQC includes various approaches to cryptography, such as lattice-based cryptography, code-based cryptography, multivariate-based cryptography, hash-based cryptography, and isogeny-based cryptography.

The first isogeny-based cryptosystem was proposed by Couveignes in 1997 [12], and then again independently by Rostovtsev and Stolbunov in 2006 (commonly referred to as CRS) [23]. They described a non-interactive key exchange using ordinary elliptic curves. New momentum in this field came in 2011 when De Feo and Jao proposed SIDH [17], the supersingular isogeny Diffie-Hellman key exchange. A variant of this algorithm called SIKE was a promising candidate for NIST PQC standardization,[1] but it was broken in several independent papers in August 2022 [3,20,22]. In 2018, Castryck, Lange, Martindale, Panny, and Renes introduced CSIDH [6], or commutative-SIDH, a key exchange protocol that adapts CRS protocol to supersingular elliptic curves. CSIDH is not affected by the previously mentioned attacks.

Compared to other post-quantum protocols, the main advantages of isogeny-based cryptography are smaller key sizes and ciphertext sizes. On the other hand, the main disadvantage of isogeny-based protocols has been the high computational cost of encryption and decryption. These advantages and disadvantages are particularly evident in digital signatures. SQISign, introduced in 2020 [13], is among the most promising and compact isogeny-based digital signatures. It has seen some speed improvements in 2022 [14], but despite this, it is still several orders of magnitude slower than other post-quantum signature schemes.

Protocols like CRS, CSIDH or, for example, Charles, Goren and Lauter's hash function [8] share the need to compute isogenies of low degree in finite field. An isogeny can be computed from the coordinates of the points in its kernel using Vélu's formulas [26]. To improve and accelerate isogeny computation, various approaches and variants of Vélu's formulas have been proposed for different curve models, such as Montgomery curves in [11], Edwards curves [7,19], and Hessian curves [2]. An algorithm by Bernstein, De Feo, Leroux and Smith [1] reduces the cost of computation of isogeny of degree N from $\mathcal{O}(N)$ to $\widetilde{\mathcal{O}}(\sqrt{N})$ and can be applied to Huff's and general Huff's curves [27].

Radical isogenies are formulas designed for computing a chain of isogenies of the same small degree between elliptic curves over a finite field. They were first introduced by Castryck, Decru and Vercauteren in 2020 [5]. The authors showed that using radical isogeny formulas in CSIDH-512 leads to a more efficient implementation and a speed-up of 19%, see [5, Section 6]. In [5], formulas were given for $N \leq 13$, and in 2022, the same group of authors, along with Houben [4], developed a different method for finding radical isogeny formulas for a given degree N, and provided formulas for $N \leq 37$.

The concept of radical isogeny formulas was initially introduced for elliptic curves in Tate normal form. Generally, an elliptic curve over a field k and a point on that curve with an order of at least $N \geq 4$ are isomorphic to an elliptic curve of the form $E\colon y^2 + (1-c)xy - by = x^3 - bx^2$ with $b, c \in k$, and a point $P = (0,0)$ of the same order N. This form is known as the Tate normal form and it provides two coefficients, denoted b and c. Given a cyclic isogeny $\varphi\colon E \to E' = E/\langle P \rangle$, radical isogeny formulas compute points P' of order N on E' such that composition $E \xrightarrow{\varphi} E' \to E'/\langle P' \rangle$ is cyclic of degree N^2. The coordinates of P' are elements of the smallest field that contains the coefficients b and c, along with a radicand ρ that is a N-th root of a rational expression in the coefficients b and c. The elliptic curve E' and point P' are also isomorphic to an elliptic curve in Tate normal form (for example, defined with coefficients b' and c') and a point $(0,0)$ of order N. This allows us to use radical isogeny formulas again, making the process iterative. The coefficients b' and c' can be expressed as elements of the same field as P'.

[1] More information about standardization is available as `https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization`.

As a first contribution of this article, in Section 3, we will extend the notion of radical isogeny formulas to the language of modular curves. To achieve this, we will utilize enhanced elliptic curves, which are curves paired with additional torsion data and affiliated with some congruence subgroup. The aforementioned parameters from Tate normal form and the radicand ρ can all be regarded as functions on the set of equivalence classes of enhanced elliptic curves. This generalization of radical isogenies for degree N is directly related to the modular curve $X_1(N)$, congruence subgroup $\Gamma_1(N)$ and pairs of enhanced elliptic curves consisting of an elliptic curve and a point of order N.

In [21], Onuki and Moriya introduced radical isogeny formulas of degrees 3 and 4 on Montgomery curves. A Montgomery curve over a field k is an elliptic curve of the form $E\colon y^2 = x^3 + Ax^2 + x$, where $A \in k$ and $A^2 \neq 4$. The coefficient A is called the Montgomery coefficient of E. For degree 4 (degree 3 is similar), the set of equivalence classes of enhanced elliptic curves for $\Gamma_0(4)$, denoted by $S_0(4)$, is equal to the set of equivalence classes of enhanced elliptic curves for $\Gamma_1(4)$. This equality implies the existence of radical isogenies formulas for the modular curve $X_0(4)$. The Montgomery coefficient A represents a class in the set $S_0(4)$, see [21, Section 2.3]. In other words, we can say that the coefficient A describes an enhanced elliptic curve where the additional torsion data is a cyclic subgroup of order 4. The Montgomery coefficient for the curve E' can be calculated by a rational expression depending on the fourth root from $4(A+2)$ see [21, Theorem 8].

The authors of [21] explored the possibility of extending radical isogeny formulas to the modular curve $X_0(N)$ when $N \geq 5$. The idea behind this can be summarized in a few informal steps. First, take a modular curve of genus zero, such as $X_0(5)$. Then, find a parameter that specifies its set of equivalence classes of enhanced elliptic curves, find a model of a universal elliptic curve for $X_0(5)$ defined by that parameter (Tate, Montgomery, or something else) and then find a radical isogeny formula on such a curve. This approach is presented as an example, see [21, Section 4] and Section 2.5.1, that argues against the existence of radical isogeny formulas for that curve. While this example indicates that finding radical isogenies for degrees greater than 4 is maybe not possible, a general answer was left as an open problem. This article provides a solution to that open problem, i.e. in Corollary 4.3 we prove that radical isogeny formulas cannot exist on the set of equivalence classes of enhanced elliptic curves for $\Gamma_0(N)$ when $N \geq 5$.

Paper organization

Section 2 provides necessary background, including brief overview on elliptic curves, isogenies of elliptic curves, the definition of congruence subgroups, modular curves, semidirect product of groups, radical isogenies and the description of the previously mentioned open problem in Example 2.4. In the section 3 we generalize radical isogenies using modular curves. Section 4 extends the setting from Section 3 to include modular curve $X_0(N)$. In the same section Theorem 4.2 is proved, and a corollary of that theorem is a solution to the open problem from Example 2.4.

2. Preliminaries

This section will provide summary of necessary background. For more details on elliptic and modular curves refer to [24], [16] and [10, Chapter III].

2.1. **Elliptic curves.** Let k be a field. An elliptic curve E over k is a smooth projective curve of genus one with a specified base point $\mathcal{O}_E$. Group of all the points on E defined over k is denoted by $E(k)$. Given an integer N, multiplication by N map is denoted with $[N]$. The kernel of this map is the N torsion subgroup, $E[N] = \{P \in E(\overline{k})\colon [N]P = \mathcal{O}_E\}$. A point P on the curve E is of order N if $[N]P = \mathcal{O}_E$ and $[m]P \neq \mathcal{O}_E$ for $m < N$. For a curve E as above and a point P of order $N \geq 4$, the following Lemma holds:

Lemma 2.1. *Let E be an elliptic curve over k and let $P \in E(k)$ be a point of order $N \geq 4$, then the pair (E, P) is isomorphic to a unique pair of the form*

$$E\colon y^2 + (1-c)xy - by = x^3 - bx^2,\ P = (0,0) \tag{2.1}$$

with $b, c \in k$ and

$$\Delta(b,c) = b^3(c^4 - 8bc^2 - 3c^3 + 16b^2 - 20bc + 3c^2 + b - c) \neq 0.$$

Curve E in (2.1) is said to be in Tate normal form. For proof see [25, Lemma 2.1].

If $\operatorname{char}(k) \nmid N$, we can define the Tate pairing as a bilinear map

$$t_N\colon E(k)[N] \times E(k)/NE(k) \to k^*/(k^*)^N\colon (P_1, P_2) \mapsto t_N(P_1, P_2),$$

where $E(k)[N]$ consists of all the points in $E[N]$ defined over k.

Following [24, Chapter II.3], a divisor for a curve E is defined as a formal sum $\sum_{P \in E} n_P(P)$, where $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many $P \in E$. A Miller function f_{N,P_1} is any function on E with divisor $N(P_1) - N(\mathcal{O}_E)$. The support of a divisor is the set of points $P \in E$ for which $n_P \neq 0$. Let D be a k-rational divisor on E that is linearly equivalent to $(P_2) - (O_E)$ and whose support is disjoint from $\{P_1, \mathcal{O}_E\}$. The support of this divisor is disjoint from the divisor of Miller function f_{N,P_1}, thus $f_{N,P_1}(D) = \prod_{P \in E} f_{N,P_1}(P)^{n_P}$ is well-defined. Then, the Tate pairing can be calculated as $t_N(P_1, P_2) = f_{N,P_1}(D)$. Furthermore, if $P_1 \neq P_2$ and the Miller function is normalized, the Tate pairing $t_N(P_1, P_2)$ is equal to $f_{N,P_1}(P_2)$. When $f_{N,P}$ is a Miller function as above and P point of order N, there exists a function $g_{N,P} \in \overline{k}(E)$ such that

$$f_{N,P} \circ [N] = g_{N,P}^N. \tag{2.2}$$

The function $g_{N,P}$ can be used to define the Weil pairing, see [24, Chapter III.8] for details.

2.2. **Isogenies of elliptic curves.** Let E and E' be elliptic curves over k. An isogeny $\varphi\colon E \to E'$ is a non-constant morphism satisfying $\varphi(\mathcal{O}_E) = \mathcal{O}_{E'}$. An example of an isogeny is multiplication by N. Except for the zero isogeny, every other isogeny is a finite map of curves, so there is a usual injection of function fields $\varphi^*\colon \overline{k}(E') \to \overline{k}(E)$. The degree of φ, denoted by $\deg(\varphi)$, is the degree of the finite extension $\overline{k}(E)/\varphi^*(\overline{k}(E'))$. An isogeny is separable (inseparable, purely inseparable) if this finite extension is separable (inseparable, purely inseparable). There exists a dual isogeny $\widehat{\varphi}\colon E' \to E$ for every isogeny φ. This dual isogeny satisfies $\widehat{\varphi} \circ \varphi = [\deg(\varphi)]$. A kernel of an isogeny is a finite subgroup of $E(\overline{k})$. The size of the kernel divides the degree of the isogeny, and they are equal when the isogeny is separable. Given a finite subgroup $C \subset E$ there exists a unique separable isogeny having domain E, codomain $E/\langle C \rangle$, and C as its kernel. Vélu's formulas can be used to calculate this isogeny, see [5, Theorem 1] for a complete list of formulas.

2.3. **Congruence subgroups, modular and enhanced elliptic curves.** The group of 2×2 matrices with integer entries and determinant equal to 1 is

$$\mathrm{SL}_2(\mathbb{Z}) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) : a, b, c, d \in \mathbb{Z}, ad - bc = 1\}.$$

The principle congruence subgroup for $N > 0$ is defined as

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

The reduction modulo N morphism $\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$ induces a homomorphism $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ with kernel $\Gamma(N)$, thus $\Gamma(N)$ is normal subgroup in $\mathrm{SL}_2(\mathbb{Z})$ of finite index. This homomorphism is a surjection, so there is an induced isomorphism

$$\mathrm{SL}_2(\mathbb{Z})/\Gamma(N) \xrightarrow{\sim} \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Other standard congruence subgroups are

$$\Gamma_1(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})\colon \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \pmod N\},$$
$$\Gamma_0(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})\colon \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \pmod N\}.$$

These subgroups satisfy $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$.

Let $\mathcal{H} = \{\tau \in \mathbb{C}\colon \mathrm{Im}(\tau) > 0\}$ be the upper half-plane and let $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbb{Z})$ be a matrix. The action of the matrix on $z \in \mathcal{H}$ is defined by

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)(z) = \frac{az+b}{cz+d}.$$

Using this fractional linear transformation, for a congruence subgroup Γ, we can define the modular curve by

$$Y(\Gamma) = \Gamma/\mathcal{H} = \{\Gamma\tau\colon \tau \in \mathcal{H}\}.$$

For $\Gamma(N), \Gamma_1(N), \Gamma_0(N)$,

$$Y(N) = \Gamma(N)/\mathcal{H}, Y_1(N) = \Gamma_1(N)/\mathcal{H} \text{ and } Y_0(N) = \Gamma_0(N)/\mathcal{H}.$$

If the action is extended to $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$, following modular curves can be defined

$$X(\Gamma) = \Gamma/\mathcal{H}^*, X(N) = \Gamma(N)/\mathcal{H}^*, X_1(N) = \Gamma_1(N)/\mathcal{H}^* \text{ and } X_0(N) = \Gamma_0(N)/\mathcal{H}^*.$$

Let E be an elliptic curve over algebraically closed field whose characteristic does not divide N. An enhanced elliptic curve for $\Gamma_0(N)$ is an ordered pair (E, C), where C is a cyclic subgroup of E of order N. Two enhanced elliptic curves (E, C) and (E', C') are equivalent if there exists an isomorphism $E \xrightarrow{\sim} E'$ that takes C to C'. We denote the set of equivalence classes of enhanced elliptic curves for $\Gamma_0(N)$ by

$$S_0(N) = \{\text{enhanced elliptic curves for } \Gamma_0(N)\}/\sim.$$

Similarly, an enhanced elliptic curve for $\Gamma_1(N)$ is a pair (E, P), where P is a point of order N. Two enhanced elliptic curves $(E, P), (E', P')$ are equivalent if there exists an isomorphism $E \xrightarrow{\sim} E'$ that takes P to P'. We denote the set of equivalence classes of enhanced elliptic curves for $\Gamma_1(N)$ by

$$S_1(N) = \{\text{enhanced elliptic curves for } \Gamma_1(N)\}/\sim.$$

Following [16, Chapter 1.3], we can define the complex elliptic curve E_τ as the quotient of the complex plane by the lattice

$$E_\tau := \mathbb{C}/\Lambda_\tau = \{z + \Lambda_\tau\colon z \in \mathbb{C}\},$$

where $\Lambda_\tau = \mathbb{Z} \oplus \tau\mathbb{Z}$. Definition of the sets $S_0(N)$ and $S_1(N)$ from the previous paragraph remains unchanged when the underlying field is $\mathbb{C}$ and E is a complex elliptic curve. Points of $Y_1(N)$ are in bijection with isomorphism classes of pairs $(E, P) \in S_1(N)$. To establish this bijection, to $\tau \in \mathcal{H}$, associate the pair $(E_\tau, \frac{1}{N}+\Lambda_\tau)$. Any pair (E, P) is isomorphic to $(E_\tau, \frac{1}{N}+\Lambda_\tau)$ for some $\tau \in \mathcal{H}$ and E_τ is isomorphic to $E_{\tau'}$ if and only if $\tau' \in \Gamma_1(N)\tau$. We have the following theorem.

Theorem 2.2. *Let N be a positive integer. The moduli space for $\Gamma_1(N)$ is*

$$S_1(N) = \{[E_\tau, \frac{1}{N} + \Lambda_\tau]\colon \tau \in \mathcal{H}\}.$$

Two points $[E_\tau, \frac{1}{N} + \Lambda_\tau]$ and $[E_{\tau'}, \frac{1}{N} + \Lambda_{\tau'}]$ are equal if and only if $\Gamma_1(N)\tau = \Gamma_1(N)\tau'$. Thus, there is a bijection

$$\psi_1\colon S_1(N) \xrightarrow{\sim} Y_1(N), \quad [\mathbb{C}/\Lambda_\tau, \frac{1}{N} + \Lambda_\tau] \mapsto \Gamma_1(N)\tau.$$

Proof. See [16, Theorem 1.5.1.]. □

Theorem 2.2 has analogous versions for congruence subgroups $\Gamma_0(N)$ and $\Gamma(N)$, also part of the [16, Theorem 1.5.1.].

2.4. **Semidirect product of groups.** Following [9], for two groups G_1 and G_2 and an action $\widehat{\varphi}\colon G_2 \to \mathrm{Aut}(G_1)$ of G_2 on G_1 (by automorphisms), the corresponding semidirect product $G_1 \rtimes_{\widehat{\varphi}} G_2$ is defined as a set

$$G_1 \times G_2 = \{(g_1, g_2)\colon g_1 \in G_1, g_2 \in G_2\},$$

where the group law on $G_1 \rtimes_{\widehat{\varphi}} G_2$ is

$$(g_1, g_2)(g_1', g_2') = (g_1 \widehat{\varphi}_{g_2}(g_1'), g_2 g_2').$$

Element (e_{G_1}, e_{G_2}) is the identity, and inverse for an element (g_1, g_2) is

$$(g_1, g_2)^{-1} = (\widehat{\varphi}_{g_2^{-1}}(g_1^{-1}), g_2^{-1}) = ((\widehat{\varphi}_{g_2^{-1}}(g_1))^{-1}, g_2^{-1}).$$

Examples of subgroups are $G_1 \times e_{G_2} = \{(g_1, e_{G_2})\colon g_1 \in G_1\}$ which is a normal subgroup, and $e_{G_1} \times G_2 = \{(e_{G_1}, g_2)\colon g_2 \in G_2\}$.

2.5. **Radical isogenies.** Following [5], this section will provide a necessary background on radical isogenies. Let k be a field, $N \geq 4$ such that $\mathrm{char}(k) \nmid N$. Consider an elliptic curve E over k and a point $P \in E(k)$ of order N. Using Lemma 2.1, the curve-point pair (E, P) is isomorphic to a unique pair of a curve

$$y^2 + (1 - c)xy - by = x^3 - bx^2,$$

where $b, c \in k$, and a point $(0, 0)$ of order N. There exists an isogeny $\varphi\colon E \to E/\langle P\rangle$ with $\langle P\rangle$, a cyclic subgroup generated by the point P, as a kernel. We denote curve $E/\langle P\rangle$ over k by E' and let P' be a point on E' of order N such that $\widehat{\varphi}(P') = P$, where $\widehat{\varphi}$ is a dual isogeny of φ. The point P' satisfying this condition is called P-distinguished and it is not unique. According to [5, Theorem 5] the coordinates of the point P' can be expressed using a formula that depends on b, c and $\sqrt[N]{\rho}$, where ρ is a representative of Tate pairing $t_N(P, -P)$. Hence, the point P' is defined over $k(b, c, \sqrt[N]{\rho})$. As P' is of order N on curve E', a Tate normal form for this pair can be defined by the unique coefficients b' and c'. The iterative process of radical isogeny formulas can be repeated on pair (E', P'). Moreover, the formulas for b' and c' can be expressed directly as elements of the field extension $k(b, c, \sqrt[N]{\rho})$, which is a simple radical[2] extension of $k(b, c)$. The explicit radical isogeny formulas when $N = 5$, are written in the following example:

Example 2.3 ([5, Section 4])**.** *Let $N = 5$. Elliptic curve E is of the form*

$$y^2 + (1 - b)xy - by = x^3 - bx^2,$$

and, using Vélu's formulas, curve E' is equal to

$$y^2 + (1 - b)xy - by = x^3 - bx^2 - 5b(b^2 + 2b - 1)x - b(b^4 + 10b^3 - 5b^2 + 15b - 1).$$

With some details omitted, $\rho = f_{5,P}(-P) = b, \alpha = \sqrt[5]{\rho}$ and point P' has coordinates

$$x_0' = 5\alpha^4 + (b - 3)\alpha^3 + (b + 2)\alpha^2 + (2b - 1)\alpha - 2b,$$
$$y_0' = 5\alpha^4 + (b - 3)\alpha^3 + (b^2 - 10b + 1)\alpha^2 + (13b - b^2)\alpha - b^2 - 11b.$$

After translating point P' to $(0, 0)$, isomorphic curve in Tate normal form will be

$$E'\colon y^2 + (1 - b')xy - b'y = x^3 - b'x^2,$$

where

$$b' = \alpha\frac{\alpha^4 + 3\alpha^3 + 4\alpha^2 + 2\alpha + 1}{\alpha^4 - 2\alpha^3 + 4\alpha^2 - 3\alpha + 1}$$

[2] A field extension $K \subset L$ is a simple radical extension of degree $N \geq 2$ if there exists an α such that $L = K(\alpha), \alpha^N \in K$, and $x^N - \alpha^N \in K[x]$ is irreducible.

and the process can be repeated.

The standard method of calculating isogenies requires a point of a particular order for each isogeny in the chain. With radical isogeny formulas, such a point is only required for the initial step, i.e. the one step that uses Vélu's formulas. Subsequent steps can be calculated without any knowledge of torsion points. The list of formulas for radicand ρ for $N \leq 13$ can be found in [5, Section 5] and link to a repository containing formulas for prime powers $16 < N \leq 37$ can be found in [4, Section 4.3].

2.5.1. **Radical isogenies on Montgomery curves.** In [21], Onuki and Moriya introduced radical isogeny formulas on Montgomery curves of degrees 3 and 4. A Montgomery curve over a field k is an elliptic curve of the form

$$E\colon y^2 = x^3 + Ax^2 + x,$$

where $A \in k$ and $A^2 \neq 4$. The coefficient A determines a class of enhanced elliptic curve $(E, (0, 0))$ in the set $S_0(4)$, see [21, Section 2.3] for details. Applying radical isogeny formulas on elements of set $S_1(N)$, i.e. on an enhanced elliptic curve (E, P), results in a curve-point pair that is also an element of $S_1(N)$. When $N = 3$ or 4, the equality $S_0(N) = S_1(N)$ holds, and the existence of radical isogeny formulas on $S_1(3)$ and $S_1(4)$ implies a radical isogeny formula on $S_0(3)$ and $S_0(4)$, respectively. This means that there is a formula between Montgomery coefficients of curves, see [21, Section 3]. However, the methods used in [21] for cases $N = 3$ or 4 cannot be directly applied to case $N \geq 5$, partly because $S_0(N) \neq S_1(N)$. Moreover, developing radical isogeny formulas on $S_0(N)$ when $N \geq 5$ might not be possible, as illustrated by the following example.

Example 2.4 ([21, Section 4]). *Let $N = 5$. Let k be a field with char$(k) \nmid N$, and E, E' two elliptic curves over the field k given in Tate normal form:*

$$E\colon y^2 + (1-b)xy - by = x^3 - bx,$$
$$E'\colon y^2 + (1-b')xy - b'y = x^3 - b'x.$$

Points $(0, 0)$ are of order 5 on these curves. The cyclic subgroup of E generated by point $(0, 0)$ is

$$\{\mathcal{O}_E, (0, 0), (b, b^2), (b, 0), (0, b)\}.$$

Pairs $(E, (0, 0))$ and $(E', (0, 0))$ are equivalent if and only if $b = b'$, while pairs $(E, \langle (0, 0)\rangle)$ and $(E', \langle (0, 0)\rangle)$ are equivalent if and only if $b = b'$ or $b = -\frac{1}{b'}$. From this we have $\frac{b^2-1}{b} = \frac{b'^2-1}{b'}$, thus $\frac{b^2-1}{b}$ is a parametrization of $S_0(5)$. From radical isogeny formula we know that b' is a rational expression in a fifth root of b, i.e. $\mathbb{Q}(b') = \mathbb{Q}(\sqrt[5]{b})$. Let $\beta = \frac{b^2-1}{b}$ and $\beta' = \frac{b'^2-1}{b'}$. Field extension $\mathbb{Q}(b)/\mathbb{Q}(\beta)$ is of degree 2. Adjoining to the field extension $\mathbb{Q}(b')/\mathbb{Q}(\beta)$ a primitive fifth root of unity $\zeta_5 \in \mathbb{C}$, we obtain a Galois extension $\mathbb{Q}(\zeta_5)(b')/\mathbb{Q}(\zeta_5)(\beta)$ of degree 10. Galois group of this extension Gal$(\mathbb{Q}(\zeta_5)(b')/\mathbb{Q}(\zeta_5)(\beta))$ is generated by automorphisms $\sigma\colon b' \mapsto -\frac{1}{b'}$ and $\tau\colon b' \mapsto \zeta_5 b'$. The fixed field of σ is $\mathbb{Q}(\zeta_5)(\beta')$, and of τ is $\mathbb{Q}(\zeta_5)(b)$. Because $\tau^{-1}\sigma\tau \neq \sigma$, the group $\langle\sigma\rangle$ is not a normal subgroup of Galois group Gal$(\mathbb{Q}(\zeta_5)(b')/\mathbb{Q}(\zeta_5)(\beta))$, thus extension $\mathbb{Q}(\zeta_5)(\beta')/\mathbb{Q}(\zeta_5)(\beta)$ cannot be a Galois extension.

If the parameter β' from Example 2.4 could be expressed as a rational expression depending on the parameter β, we would have a direct and simpler way (quadratic equation) to calculate b', rather than the radical isogeny formulas. However, since the field extension $\mathbb{Q}(\zeta_5)(\beta')/\mathbb{Q}(\zeta_5)(\beta)$ is not a Galois extension, this is not possible. Nevertheless, it may be possible to find a different β', i.e. a different parametrization of $S_0(5)$ which will make the field extension $\mathbb{Q}(\zeta_5)(\beta')/\mathbb{Q}(\zeta_5)(\beta)$ Galois.

3. Radical isogenies in the language of modular curves

Throughout this section we are using the same notation introduced in Section 2.5, E is the starting elliptic curve over a field k, $N \geq 4$ such that $\mathrm{char}(k) \nmid N$, $P \in E(k)$ a point of order N, E' a curve over k defined with $E/\langle P\rangle$, $\varphi\colon E \to E'$ an isogeny with kernel equal to $\langle P\rangle$ and P' a point of order N on E' such that $\widehat{\varphi}(P') = P$.

We will continue to work with enhanced elliptic curves for different congruence subgroups. For any elliptic curve $\widetilde{E}$ and point $\widetilde{P}$ of order $N \geq 4$, let its unique Tate normal form be defined with parameters $\widetilde{b}$ and $\widetilde{c}$. Let $\mathbf{b}$ denote a mapping $(\widetilde{E}, \widetilde{P}) \mapsto \widetilde{b}$, i.e. $\mathbf{b}$ is a function on the set of the enhanced elliptic curves for $\Gamma_1(N)$, such that for a curve $(\widetilde{E}, \widetilde{P})$ it returns parameter $\widetilde{b}$ from corresponding Tate normal form. This is a well-defined function because Tate's normal form is unique. Analogously, for parameter $\widetilde{c}$, function $\mathbf{c}\colon (E, P) \mapsto c$ is well-defined. Definition of modular functions on enhanced elliptic curves implies that $\mathbf{b}$ and $\mathbf{c}$ are elements of $k(X_1(N))$. For curves E and E' we have $(E,P) \overset{\mathbf{b}}{\mapsto} b$, $(E,P) \overset{\mathbf{c}}{\mapsto} c$, $(E',P') \overset{\mathbf{b}}{\mapsto} b'$ and $(E',P') \overset{\mathbf{c}}{\mapsto} c'$. We would like to connect parameters b, c with b', c' using modular curves and maps on them. The following sequence of maps will be considered:

$$\begin{aligned} (E,P) &\to (E',P') \overset{\mathbf{b}}{\mapsto} b', \\ (E,P) &\to (E',P') \overset{\mathbf{c}}{\mapsto} c'. \end{aligned} \tag{3.1}$$

Since the point P' is not unique, the map $(E,P) \to (E',P')$ is not uniquely defined, and therefore is no obvious connection on $X_1(N)$. For a point P of order N, let R be a point on curve E of order N^2 such that $[N]R = P$. This point R is not unique. The pair (E,R) is an enhanced elliptic curve for $\Gamma_1(N^2)$. Let P' be an image of a point R under the isogeny φ, i.e.

$$P' := \varphi(R) = R + \langle P\rangle.$$

This is a point of order N on the curve E'. Since we have

$$\hat{\varphi}(P') = \hat{\varphi}(\varphi(R)) = [\deg\ \varphi]R = [N]R = P,$$

point P' is P-distinguished. We can modify the sequence of maps in (3.1) and continue to work with parameter b and associated functions, as the approach for c is the same. Beginning with the enhanced elliptic curve (E,R), we have the following maps:

$$(E,R) \to (E,[N]R) = (E,P) \overset{\mathbf{b}}{\mapsto} b, \tag{3.2}$$

$$(E,R) \to (E/\langle [N]R\rangle, R + \langle [N]R\rangle) = (E/\langle P\rangle, R + \langle P\rangle) = (E',P') \overset{\mathbf{b}}{\mapsto} b'. \tag{3.3}$$

Using the mappings described in (3.3), we can, similar to $\mathbf{b}$, define a function $\mathbf{b}'\colon (E,R) \mapsto b'$, which is a function on the set of enhanced elliptic curves for $\Gamma_1(N^2)$. Maps and functions are visualized in Figure 1.

The connection between parameters b and b' can now be extended to an enhanced elliptic curve (E,R), i.e. to functions in $X_1(N^2)$. For every N, let $\pi_{1,N}$ and $\pi_{2,N}$ define a pair of pullback operators:

$$\begin{aligned} &\pi_{1,N}^*\colon k(X_1(N)) \to k(X_1(N^2)),\ \pi_{1,N}((E,R)) = (E,[N]R), \\ &\pi_{2,N}^*\colon k(X_1(N)) \to k(X_1(N^2)),\ \pi_{2,N}((E,R)) = (E/\langle [N]R\rangle, R + \langle [N]R\rangle). \end{aligned}$$

From

$$(\pi_{1,N}^*\mathbf{b})(E,R) = \mathbf{b}(\pi_{1,N}(E,R)) = \mathbf{b}(E,[N]R) = \mathbf{b}(E,P)$$

and

$$(\pi_{2,N}^*\mathbf{b})(E,R) = \mathbf{b}(\pi_{2,N}(E,R)) = \mathbf{b}(E/\langle [N]R\rangle, R + \langle [N]R\rangle) = \mathbf{b}(E',P') = \mathbf{b}'(E,R),$$

$$\begin{tikzcd}
X_1(N^2), \Gamma_1(N^2) \arrow[r, squiggly, no head] & (E,R) \arrow[d, "N\cdot"'] \arrow[dr, "\varphi"] & \\
& (E,[N]R) \arrow[d, equal] & (E/\langle [N]R\rangle, R+\langle [N]R\rangle) \arrow[d, equal] \\
X_1(N), \Gamma_1(N) \arrow[r, squiggly, no head] & (E,P) \arrow[d, "\mathbf{b}"] & (E',P') \arrow[d, "\mathbf{b}"] \\
& b & b'
\end{tikzcd}$$

Figure 1. Maps on enhanced elliptic curves

we can identify $\mathbf{b}$ and $\mathbf{b}'$ with their respective pullbacks by $\pi_{1,N}$ and $\pi_{2,N}$ and define

$$b := \pi_{1,N}^*\mathbf{b} \text{ and } b' := \pi_{2,N}^*\mathbf{b}$$

as functions on $X_1(N^2)$. Function b' is an element of $\pi_{2,N}^*(k(X_1(N)))$, so if proved that there exist some modular function g in $k(X_1(N^2))$, defined using b and c, such that

$$\pi_{1,N}^*(k(X_1(N)))(g) = \pi_{2,N}^*(k(X_1(N))), \tag{3.4}$$

b' will also be an element of $\pi_{1,N}^*(k(X_1(N)))(g)$.

Let P be a point of order N as before, and let $f_{N,P}$ be a normalized Miller function. With the value of $f_{N,P}$ at point $-P$, we can define a modular function f on the set of enhanced elliptic curves for $\Gamma_1(N)$ as:

$$f\colon (E,P) \mapsto f_{N,P}(-P) \in k(X_1(N)).$$

For the function $f_{N,P}$ and the point P, from equation (2.2), there exists a function $g_{N,P} \in \overline{k}(E)$ such that $f_{N,P} \circ [N] = g_{N,P}^N$. Using this equality, for an enhanced elliptic curve (E,R), where, as before, $P = [N]R$, we have a function on $X_1(N^2)$ given by

$$\begin{aligned}(E,R) \mapsto f_{N,[N]R}(-[N]R) &= f_{N,[N]R}([N](-R)) \\ &= g_{N,[N]R}(-R)^N = g_{N,P}(-R)^N.\end{aligned}$$

The function g defined as $g := (E,R) \mapsto g_{N,P}(-R) \in k(X_1(N^2))$ satisfies the property

$$g^N = f,$$

which means that the N-th root of f is a function on $X_1(N^2)$. Both functions b, b', as well as function g are elements of $k(X_1(N^2))$. However, due to the large size of this field, it is currently impossible to prove (3.4). Thus, it is necessary to identify a smaller quotient of $X_1(N^2)$ where b, b', and g are well-defined.

3.1. **"Shrinking" the field of definition.**

To gain a better understanding of the function b', we will investigate the preimages of (E,P) under the pullback operator $\pi_{2,N}$. Specifically, we will investigate pairs (E,R) and (E,R') that are mapped by $\pi_{2,N}$ to the same point $(E/\langle [N]R\rangle, R + \langle [N]R\rangle)$. For the equality

$$(E/\langle [N]R'\rangle, R' + \langle [N]R'\rangle) = (E/\langle [N]R\rangle, R + \langle [N]R\rangle)$$

to hold, we require $\langle [N]R'\rangle = \langle [N]R\rangle$ and $R' + \langle [N]R'\rangle = R + \langle [N]R\rangle$. Combining these conditions, we get $R' + \langle [N]R\rangle = R + \langle [N]R\rangle$, which implies that there exists some $l \in \mathbb{Z}/N\mathbb{Z}$ such that

$$R' = R + [l]\cdot([N]R) \text{ and } [N]R' = [N](R + [l]P).$$

Therefore, we have

$$\langle [N](R+[l]P)\rangle = \langle [N]R\rangle.$$

Since point R has order N^2, the points $(E,R),(E,R+[1\cdot N]R),\dots,(E,R+[(N-1)\cdot N]R)$ are all mapped to the same final point. From the definition of b', it is apparent that it is a function on $X_1(N^2)$ that maps points of this form to the same final point.

Let t_m be an operator on $S_1(N^2)$ defined as $t_m\colon (E,\overline{P}) \mapsto (E,[m]\overline{P})$. When $m = N+1$, define $t := t_{N+1}$. On an enhanced elliptic curve $(E,R)\in S_1(N^2)$, this operator act as follows:

$$(E,R) \overset{t}{\mapsto} (E,[N+1]R) \overset{t}{\mapsto} (E,[(N+1)^2]R) \overset{t}{\mapsto} \dots \overset{t}{\mapsto} (E,[(N+1)^{N-1}]R).$$

The order of the operator t is equal to N since we have $t^N(E,R) = (E,[(N+1)^N]R) = (E,R)$. Composing t with $\pi_{1,N}$ on the enhanced elliptic curve (E,R), we have:

$$\begin{aligned}\pi_{1,N}(t(E,R)) &= \pi_{1,N}(E,[N+1]R)\\ &= (E,[N(N+1)]R) \text{ (since order of } R \text{ is } N^2)\\ &= (E,[N]R)\\ &= \pi_{1,N}(E,R),\end{aligned}$$

and for $\pi_{2,N}$:

$$\begin{aligned}\pi_{2,N}(t(E,R)) &= \pi_{2,N}(E,[N+1]R)\\ &= (E/\langle [N(N+1)]R\rangle, [N+1]R+\langle [N(N+1)]R\rangle)\\ &= (E/\langle [N]R\rangle, R+\langle [N]R\rangle) \text{ (since } [N]R\in\langle [N]R\rangle)\\ &= \pi_{2,N}(E,R),\end{aligned}$$

thus, every pullback by $\pi_{1,N}$ or by $\pi_{2,N}$ will be invariant under t. Modular function $(E,R) \overset{g}{\mapsto} g_{N,P}(-R)$, with property $g^N = f$, is also invariant under t. Referring again to [24, Chapter III.8] for more details, function $g_{N,[N]R}$ can be used to define Weil pairing

$$e_N(S,P) = \frac{g_{N,[N]R}(X+S)}{g_{N,[N]R}(X)},$$

where $X\in E$ and $S,P\in E[N]$ with $S=P$ allowed, and as before, we have $P=[N]R$. To see that function g is invariant under t, let $(E,R)\in S_1(N^2)$, then

$$\begin{aligned}t(E,R) = (E,[N+1]R) \overset{g}{\mapsto} g_{N,[N(N+1)]R}&(-[N+1]R)\\ = g_{N,[N]R}&(-[N]R-R)\\ = g_{N,[N]R}&(-R-P)\end{aligned}$$

and together with the bilinearity and alternating property of Weil pairing,

$$\begin{aligned}g_{N,[N]R}(-R-P) &= g_{N,[N]R}(-R)e_N(-P,P) = g_{N,[N]R}(-R)e_N([N]P,P)\\ &= g_{N,[N]R}(-R)e_N(P,P)^{N-1} = g_{N,[N]R}(-R) = g_{N,P}(-R).\end{aligned}$$

Let $\langle t\rangle$ denote the group of automorphisms of $X_1(N^2)$ generated by t. A function on $X_1(N^2)$ that is invariant under the operator t can be viewed as a function on the quotient $X_1(N^2)/\langle t\rangle$. As discussed above, b' is an example of such a function. The quotient $X_1(N^2)/\langle t\rangle$, i.e. the quotient of modular curve with the operator, is again a modular curve. To see this, following [18] and [15] we can assume, for a field k defined at the beginning of this section, that $k=\mathbb{C}$. Then, we have the following proposition, which explicitly calculates the congruence subgroup defining this quotient, i.e. corresponding modular curve.

Proposition 3.1. *Let t be an operator defined on the set of enhanced elliptic curves for $\Gamma_1(N^2)$ with $t(E,R)=(E,[N{+}1]R)$. Let $\langle t\rangle$ denote the subgroup of automorphisms of $X_1(N^2)$ generated by t. The quotient of the extended upper half-plane $\mathcal{H}^*=\mathcal{H}\cup\mathbb{Q}\cup\{\infty\}$ and the congruence subgroup*

$$\widetilde{\Gamma}(N):=\left\{\left(\begin{smallmatrix} a & b\\ c & d\end{smallmatrix}\right)\in \mathrm{SL}_2(\mathbb{Z})\colon c\equiv 0\ (mod\ N^2),\ a,d\equiv 1\ (mod\ N)\right\},$$

i.e. $\widetilde{\Gamma}(N)/\mathcal{H}^*$, is a modular curve consisting of all the functions on $X_1(N^2)$ invariant under t.

Proof. As shown in [16, Section 1.5], sets of equivalence classes of enhanced elliptic curves can be used to describe the quotients of the upper half-plane by congruence subgroups. In other words, for a function f on $X_1(N^2)/\langle t\rangle$, there is a corresponding meromorphic function $\mathbf{f}$ on the upper half-plane that is invariant under the action of $\Gamma_1(N^2)$ and a matrix $\mathbf{t}\in \mathrm{SL}_2(\mathbb{Z})$ corresponding to the operator t. To see this, note that Theorem 2.2 shows that $S_1(N^2)$ is a moduli space of isomorphism classes of complex elliptic curves and N^2-torsion data, i.e.

$$S_1(N^2)=\{[E_\tau,\frac{1}{N^2}+\Lambda_\tau]\},$$

where τ,Λ_τ and E_τ are defined as in Section 2. Describing what the operator t does in the sense of congruence subgroup implies working with the pair (E,R) after applying the operator t, i.e. with

$$t(E_\tau,\frac{1}{N^2}+\Lambda_\tau)=(E_\tau,\frac{N+1}{N^2}+\Lambda_\tau).$$

We need to find $\tau'\in\mathcal{H}$, such that $(E_\tau,\frac{N+1}{N^2}+\Lambda_\tau)$ is isomorphic to $(E_{\tau'},\frac{1}{N^2}+\Lambda_{\tau'})$. Let $\tau'=\frac{(1-N)\tau-1}{N^2\tau+1+N}$ and $\Lambda_{\tau'}=\langle 1,\tau'\rangle$. Elements 1 and τ are linear combination of 1 and τ', which is obvious for 1, and for τ we have:

$$(1+N)(N^2\tau+N+1)\cdot\frac{(1-N)\tau-1}{N^2\tau+N+1}+(N^2\tau+N+1)\cdot 1=\tau.$$

From this, $\Lambda_{\tau'}$ is isomorphic to Λ_τ. Moreover, for the matrix

$$\mathbf{t}=\left(\begin{smallmatrix} 1-N & -1\\ N^2 & 1+N\end{smallmatrix}\right)\in\Gamma_0(N^2)\setminus\Gamma_1(N^2),$$

using the usual fractional linear transformation on $\mathcal{H}$, we have $\mathbf{t}(\tau)=\tau'$. Desired congruence subgroup $\widetilde{\Gamma}(N)$ is generated by $\Gamma_1(N^2)$ and matrix $\mathbf{t}$, thus

$$\widetilde{\Gamma}(N)=\left\{\left(\begin{smallmatrix} a & b\\ c & d\end{smallmatrix}\right)\in \mathrm{SL}_2(\mathbb{Z})\colon c\equiv 0\ (\mathrm{mod}\ N^2),\ a,d\equiv 1\ (\mathrm{mod}\ N)\right\}.$$

It is clear from the construction of the congruence subgroup $\widetilde{\Gamma}(N)$ that the quotient $\widetilde{\Gamma}(N)/\mathcal{H}^*$ defines a modular curve consisting of all the functions on $X_1(N^2)$ invariant under t. □

As a direct consequence of Proposition 3.1, $X_1(N^2)/\langle t\rangle$ is a well-defined modular curve with a function field equal to

$$k(X_1(N^2)/\langle t\rangle)=\{f\in k(X_1(N^2))\colon f(t(E,R))=f(E,R),\forall (E,R)\in S_1(N^2)\}.$$

The following proposition shows the relationship between the congruence subgroups $\widetilde{\Gamma}(N)$ and $\Gamma_1(N^2)$.

Proposition 3.2. *Let $\widetilde{\Gamma}(N)$ be a congruence subgroup defined as*

$$\widetilde{\Gamma}(N)=\left\{\left(\begin{smallmatrix} a & b\\ c & d\end{smallmatrix}\right)\in \mathrm{SL}_2(\mathbb{Z})\colon c\equiv 0\ (mod\ N^2),\ a,d\equiv 1\ (mod\ N)\right\}.$$

The congruence subgroup

$$\Gamma_1(N^2)=\{\left(\begin{smallmatrix} a & b\\ c & d\end{smallmatrix}\right)\in \mathrm{SL}_2(\mathbb{Z})\colon \left(\begin{smallmatrix} a & b\\ c & d\end{smallmatrix}\right)\equiv\left(\begin{smallmatrix} 1 & *\\ 0 & 1\end{smallmatrix}\right)\ (mod\ N^2)\}$$

is a normal subgroup of $\widetilde{\Gamma}(N)$ with index N.

Proof. The congruence subgroup $\widetilde{\Gamma}(N)$ is generated with the congruence subgroup $\Gamma_1(N^2)$ and matrix $\mathbf{t} = \left(\begin{smallmatrix} 1-N & -1 \\ N^2 & 1+N \end{smallmatrix}\right) \in \Gamma_0(N^2) \setminus \Gamma_1(N^2)$. To prove that $\Gamma_1(N^2)$ is a normal subgroup of $\widetilde{\Gamma}(N)$ it is enough to see that $\mathbf{t}^{-1} \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mathbf{t} \in \Gamma_1(N^2)$, for every matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(N^2)$. This is true because

$$\begin{aligned}
&\left(\begin{smallmatrix} 1-N & -1 \\ N^2 & 1+N \end{smallmatrix}\right)\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} 1+N & 1 \\ -N^2 & 1-N \end{smallmatrix}\right) = \\
&\qquad = \left(\begin{smallmatrix} a(1-N)(N+1)+c(1-N)+N^2(b(N+1)+d) & -a(N+1)+b(N+1)(N+1)+d(N+1)-c \\ c(1-N)^2-aN^2(1-N)+N^2(d(1-N)-bN^2) & aN^2+d(1-N)(N+1)-bN^2(N+1)-c(1-N)) \end{smallmatrix}\right) \\
&\qquad \equiv \left(\begin{smallmatrix} 1 & 2(N+1)+b(2N+1) \\ 0 & 1 \end{smallmatrix}\right) \pmod{N^2}.
\end{aligned}$$

To calculate the index of $\Gamma_1(N^2)$ in $\widetilde{\Gamma}(N)$ we will use the homomorphism $\pi_N \colon \mathrm{SL}(\mathbb{Z}) \to \mathrm{SL}(\mathbb{Z}/N\mathbb{Z})$, induced by the reduction modulo N for $N \geq 1$. The kernel of π_N is the principal congruence subgroup $\Gamma(N)$, which is a normal subgroup of finite index in $\mathrm{SL}(\mathbb{Z})$. Any other congruence subgroup $\Gamma(N) \subset \widetilde{\Gamma}$ is of finite index in $\mathrm{SL}(\mathbb{Z})$ and it is a preimage of π_N, i.e. $\widetilde{\Gamma} = \pi_N^{-1}(\widehat{\Gamma})$ where $\widehat{\Gamma}$ is some subgroup of $\mathrm{SL}(\mathbb{Z}/N\mathbb{Z})$. The index $[\widetilde{\Gamma} \colon \Gamma(N)]$ is equal to $\#\widehat{\Gamma}$.

For $\#\widehat{\widetilde{\Gamma}(N)}$, after reducing elements of $\widetilde{\Gamma}(N)$ modulo N^2, the conditions on elements are $c = 0, a, d \equiv 1 \pmod{N}$ and $a, b, c, d \in \mathbb{Z}/N^2\mathbb{Z}$. There are no conditions on b, but a and d must satisfy a condition for determinant $ad \equiv 1 \pmod{N^2}$. Writing $a = 1 + kN$ and $d = 1 + lN$, where $k, l \in \{0, 1, \ldots, N-1\}$, we get

$$(1 + kN)(1 + lN) = 1 + N(k + l) + klN^2 \equiv 1 \pmod{N^2},$$

which implies $k+l \equiv 0 \pmod{N}$, so l depends completely on k. Therefore, d depends completely on a. Altogether, $\#\widehat{\widetilde{\Gamma}(N)} = N^3$. The index $[\widetilde{\Gamma}(N) \colon \Gamma(N^2)]$ is equal to $[\widetilde{\Gamma}(N) \colon \Gamma_1(N^2)][\Gamma_1(N^2) \colon \Gamma(N^2)]$, thus

$$[\widetilde{\Gamma}(N) \colon \Gamma_1(N^2)] = \frac{\#\widehat{\widetilde{\Gamma}(N)}}{[\Gamma_1(N^2) \colon \Gamma(N^2)]} = \frac{\#\widehat{\widetilde{\Gamma}(N)}}{N^2} = \frac{N^3}{N^2} = N.$$

□

By performing a calculation similar to the one used in the proof of Proposition 3.2, it can be shown that the index of $[\Gamma_1(N) \colon \Gamma_1(N^2)]$ is equal to N^2. Let $k(X_1(N^2))$ denote the function field corresponding to the modular curve $X_1(N^2)$. Using the results of the Proposition 3.2, the quotient $\widetilde{\Gamma}(N)/\Gamma_1(N^2)$ acts as a group of automorphism of $k(X_1(N^2))$ with fixed field $k(X(\widetilde{\Gamma}(N)))$, i.e.

$$k(X(\widetilde{\Gamma}(N))) = k(X_1(N^2))^{\widetilde{\Gamma}(N)/\Gamma_1(N^2)}.$$

This gives us an equality of function fields:

$$k(X(\widetilde{\Gamma}(N))) = k(X_1(N^2))^{\mathbf{t}}.$$

So we have

$$k(X(\widetilde{\Gamma}(N))) = k(X_1(N^2)/\langle t \rangle).$$

We have shown that the function $b \in \pi_{1,N}^*(k(X_1(N)))$ is invariant under the operator t. Therefore,

$$\pi_{1,N}^*(k(X_1(N))) \overset{N}{\subset} k(X(\widetilde{\Gamma}(N))) = k(X_1(N^2)/\langle t \rangle),$$

where the degree of the extension is equal to the index of the subgroup. Returning to the equality (3.4), the modular function $g \colon (E, R) \mapsto g_{N,P}(-R)$ is an element of the field $k(X_1(N^2)/\langle t \rangle)$ with property $g^N = f$. The polynomial $x^N - f$ is a polynomial of degree N in $\pi_{1,N}^*(k(X_1(N)))[x]$ having g as a root. The equality (3.4) depends on the irreducibility of the polynomial $x^N - f$.

Lemma 3.3. *Let f be a function defined on the set $S_1(N)$ with $(E,P) \mapsto f_{N,P}(-P)$, where $f_{N,P}$ is a normalized Miller function. Let g be a function defined on the set $S_1(N^2)$ with $(E,R) \mapsto g_{N,P}(-R)$, where $P = [N]R$ and $f_{N,P} \circ [N] = g_{N,P}^N$. Let $t \in Gal(k(X_1(N^2))/k(X_1(N)))$ be an operator defined as $t(E,R) = (E,[N+1]R)$, $(E,R) \in S_1(N^2)$. Let $\pi_{1,N}^*\colon k(X_1(N)) \to k(X_1(N^2)$ be a pullback operator defined as $\pi_{1,N}((E,R)) = (E,[N]R)$. Then, the polynomial $x^N - f$ is an irreducible polynomial in $\pi_{1,N}^*(k(X_1(N)))[x]$.*

Proof. We will show that the field extension $\pi_{1,N}^*(k(X_1(N)))(g)$ has degree N over $k(X_1(N))$, i.e. that the function g is only invariant under the operator t, thus it is an element of the function field $k(X(\widetilde{\Gamma}(N)))$, and cannot be an element of some other field $k(X(\Gamma))$ with $\widetilde{\Gamma}(N) \subsetneqq \Gamma \subset \Gamma_1(N)$ and $g \in k(X(\Gamma))$.

Assume then that g is invariant under another operator $T \in Gal(k(X_1(N^2))/k(X_1(N)))$ such that $T(E,R) = (E,T(R))$, $(E,R) \in S_1(N^2)$, and where $NT(R) = [N]R = P$. The invariant property of the function g, together with the previously defined Weil pairing implies:

$$1 = \frac{g_{N,[N]R}(-T(R))}{g_{N,[N]R}(-R)} = \frac{g_{N,P}((R-T(R)) - R)}{g_{N,P}(-R)} = e_N(P, R - T(R)).$$

The point $R - T(R)$ belongs to $E[N]$ because, by assuming $NT(R) = [N]R = P$, we have $N(R - T(R)) = P - P = \mathcal{O}$. Therefore, $e_N(P, R - T(R))$ is consistent with the definition of Weil pairing. From this, for every $(E,R) \in S_1(N^2)$, we have $e_N(P, R - T(R)) = 1$.

Let E be a fixed elliptic curve and P be a point of order N on that curve such that $P = [N]R$. Since the Weil pairing is non-degenerate, and $e_N(P, R - T(R)) = 1$ for every R, it follows that the point $R - T(R)$ belongs to the subgroup $\langle P \rangle$. As a consequence, the point $T(R)$ can be written as $R + [l]P$ for some $l \in \mathbb{Z}$, which depends on R.

In comparison to the operator t, since g is invariant under t, we have:

$$g(E,R) = g(t(E,R)) = g(E,[N+1]R) = g(E,R+P),$$

which implies $g(E,R) = g(E,R+[k]P)$ for every $k \in \mathbb{Z}$. For the operator T, we have:

$$g(E,R) = g(E,T(R)) = g(E,R+[l]P),$$

for some $l \in \mathbb{Z}$. Therefore, the invariant property of the function g under the operator T follows from the invariant property of the function g under the operator t, which means that g is modular only for the congruence subgroup $\widetilde{\Gamma}(N)$. This implies that the function field $\pi_{1,N}^*(k(X_1(N)))(g)$ is an extension of degree exactly N over $k(X_1(N))$. The roots of the polynomial $x^N - f$ are of the form $\zeta_N^n g$, where ζ_N represents the N-th root of unity and n is a positive integer. If we assume that this polynomial is not irreducible, then we could find two non-constant polynomials $f_1, f_2 \in k(X_1(N))[x]$, such that $x^N - f = f_1(x)f_2(x)$. However, this would lead to a contradiction since g is a root for f_1 and has degree greater than or equal to N, which is the degree of g. Therefore, the polynomial $x^N - f$ is irreducible.

□

In conclusion, the irreducibility of the polynomial $x^N - f$, as stated in Lemma 3.3, implies

$$\pi_{1,N}^*(k(X_1(N)))(g) = k(X_1(N^2)/\langle t \rangle),$$

which means b' is an element of $\pi_{1,N}^*(k(X_1(N)))(g)$. Therefore, equality (3.4) holds, and it is possible to generalize radical isogenies using modular functions.

Example 3.4. *Let $N = 5$ and E be an elliptic curve over the field*

$$\mathbb{Q}_5(b,c) := Frac\ \frac{\mathbb{Q}[b,c]}{(F_5(b,c))}.$$

Tate normal form for E, together with the point P of order 5 is

$$E\colon y^2 + (1-b)xy - by = x^3 - bx^2,\ P = (0,0). \tag{3.5}$$

In general, polynomial $F_N(b,c) \in \mathbb{Z}[b,c]$ is an irreducible polynomial calculated from scalar multiples of the point P. When $N \geq 4$, condition $F_N(b,c) = 0$ together with $F_m(b,c) \neq 0$, when $4 \leq m < N$, and determinant of E not equal to zero, ensures that the point P is of order N. Other direction is also true, when P is of order N, then $F_N(b,c) = 0$. Additionally, $F_N(b,c)$ is a defining polynomial for the modular curve $X_1(N)$, so $\mathbb{Q}_N(b,c)$ is a function field of $X_1(N)$ over $\mathbb{Q}$. More details are available in [25].

In the case of $N = 5$ we have $F_5(b,c) = b - c = 0$, which implies a simpler Tate normal form (3.5). Having only a parameter b results in only one modular function $\mathbf{b}$ in $k(X_1(5))$. On the other side, the curve E' and the point P' of order 5 are given by

$$E' = E/\langle P\rangle\colon y^2 + (1-b')xy - b'y = x^3 - b'x^2,\ P' = (0,0).$$

For a point P, let R be a point of order 25 such that $[5]R = P$. The pair (E,R) is an enhanced elliptic curve for $\Gamma_1(25)$. The pullbacks $\pi_{1,5}, \pi_{2,5}$ and maps b, b' are defined as before.

From the example in [5, Section 4], when $N = 5$, $f_{5,P}(-P) = b \in \mathbb{Q}_5(b)$. The fifth root of b is a function on $X_1(25)$, as $(E,R) \overset{g}{\mapsto} g_{5,[5]R}(-R)$ is a well-defined map with a property $g^5 = b$.

Observing the preimages of $\pi_{2,5}$, points $(E,R), (E, R+[1\cdot5]R), (E, R+[2\cdot5]R), (E, R+[3\cdot5]R)$ and $(E, R+[4\cdot5]R)$ are all mapped to the same final point. The operator t defined as $t(E,R) \mapsto (E,[5+1]R) = (E,[6]R)$ is of order 5 and $\langle t\rangle$ is isomorphic to $\mathbb{Z}/5\mathbb{Z}$. The congruence subgroup generated by $\Gamma_1(25)$ and matrix $\mathbf{t} = \left(\begin{smallmatrix} -4 & -1 \\ 25 & 6 \end{smallmatrix}\right)$ is

$$\widetilde{\Gamma}(5) = \left\{ \left(\begin{smallmatrix} \tilde{a} & \tilde{b} \\ \tilde{c} & \tilde{d} \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})\colon \tilde{c} \equiv 0\ (mod\ 25),\ \tilde{a}, \tilde{d} \equiv 1\ (mod\ 5) \right\}.$$

Functions b, b', g and every pullback by $\pi_{1,5}$ or $\pi_{2,5}$ are invariant under t, so they are also defined on the quotient $X_1(25)/\langle t\rangle$. For the number of elements in group $\#\widehat{\widetilde{\Gamma}}(5)$, after reducing elements of $\widetilde{\Gamma}(5)$ modulo 25, conditions on elements are $\tilde{c} = 0, \tilde{a}, \tilde{d} \equiv 1\ (mod\ 5)$ and $\tilde{a}, \tilde{b}, \tilde{c}, \tilde{d} \in \mathbb{Z}/25\mathbb{Z}$. The only possibilities for $\tilde{a}$ and $\tilde{d}$ are from the set $\{1, 6, 11, 16, 21\}$. Since the determinant of the matrix has to be 1 in $\mathrm{SL}(\mathbb{Z}/25\mathbb{Z})$, there are 25 possibilities for $\tilde{b}$. Therefore, there are 125 elements in this group, and the index $[\widetilde{\Gamma}(5)\colon \Gamma_1(25)] = 5$. The field extension $\pi_{1,5}^*(k(X_1(5))) \subset k(X_1(25)/\langle t\rangle)$ has degree 5, polynomial $X^5 - b$ is irreducible in $\pi_{1,5}^*(k(X_1(5)))$, has a well-defined root, thus

$$\pi_{1,5}^*(k(X_1(5)))(\sqrt[5]{b}) = k(X_1(25)/\langle t\rangle),$$

meaning $b' \in \pi_{1,5}^*(k(X_1(5)))(\sqrt[5]{b})$ and b' is a rational expression of $\sqrt[5]{b}$.

4. Extending to $X_0(N)$

Continuing from the setting of the previous section, the discussion for $\Gamma_1(N)$, $X_1(N)$ and $S_1(N)$ can be extended to $\Gamma_0(N), X_0(N)$ and $S_0(N)$. Let $\boldsymbol{\beta}$ be a function on enhanced elliptic curves for $\Gamma_0(N)$, i.e. an element of $k(X_0(N))$. For example, we can take $\boldsymbol{\beta}$ to be Hauptmodul[3] for $k(X_0(N))$. Such Hauptmodul will exist if the genus of the modular curve is zero. Pullback operators $\pi_{1,N}$ and $\pi_{2,N}$ are defined as in the previous section, and ψ_N is a pullback operator defined by

$$\psi_N^*\colon k(X_0(N)) \to k(X_1(N)),\ \psi_N((E,P)) = (E, \langle P\rangle).$$

Applying the compositions $\pi_{1,N}^* \circ \psi_N^*$ and $\pi_{2,N}^* \circ \psi_N^*$ to functions from $k(X_0(N))$ results in elements of $k(X_1(N^2))$. From now on, we will identify the function $\boldsymbol{\beta}$ with $\beta := \pi_{1,N}^*(\psi_N^*(\boldsymbol{\beta}))$

[3] A Hauptmodul for a congruence subgroup Γ is a function that generates the field of modular functions for Γ.

$$\begin{tikzcd}
X_1(N^2),\Gamma_1(N^2) \arrow[r, squiggly, no head] & (E,R) \arrow[d, "\pi_{1,N}"'] \arrow[dr, "\pi_{2,N}"] & \\
X_1(N),\Gamma_1(N) \arrow[r, squiggly, no head] & (E,[N]R) \arrow[r] \arrow[d, equal] & (E/\langle [N]R\rangle, R+\langle [N]R\rangle) \arrow[d, equal] \\
 & (E,P) \arrow[d, "\psi_N"'] & (E',P') \arrow[d, "\psi_N"'] \\
X_0(N),\Gamma_0(N) \arrow[r, squiggly, no head] & (E,\langle P\rangle) \arrow[d, "\boldsymbol{\beta}"'] & (E',\langle P'\rangle) \arrow[d, "\boldsymbol{\beta}"'] \\
 & \beta(E,R) & \beta'(E,R)
\end{tikzcd}$$

FIGURE 2. Maps on enhanced elliptic curves, including $X_0(N)$

and define $\beta' := \pi_{2,N}^*(\psi_N^*(\boldsymbol{\beta}))$. Both β and β' are elements of $k(X_1(N^2))$. Maps and connections are visible in Figure 2.

Because β' is defined as pullback by π_2, as before, it is invariant under the operator t, which implies $\beta' \in k(X(\widetilde{\Gamma}(N)))$. Similarly to the previous section, if radical isogeny formulas exist on $X_0(N)$ it should be possible to express β' as an element of some function field depending on β. To this end, we are interested in preimages of (E,P), now under the maps $\pi_{1,N}^*(\psi_N^*)$ and $\pi_{2,N}^*(\psi_N^*)$, i.e. pairs of enhanced elliptic curves for $\Gamma_1(N^2), (E,R)$ and (E,R') mapped to the same final points $(E,\langle [N]R\rangle)$ and $(E/\langle [N]R\rangle, \langle R + \langle [N]R\rangle\rangle)$. Moreover, to include functions on $X_0(N)$, maps (3.2) and (3.3) are extended to

$$\begin{aligned}
&(E,R) \to (E,[N]R) = (E,P) \to (E,\langle P\rangle) \\
&(E,R) \to (E/\langle [N]R\rangle, R+\langle [N]R\rangle) = (E',P') \to (E',\langle P'\rangle).
\end{aligned} \tag{4.1}$$

Describing preimages of maps in (4.1) will result in another quotient of $X_1(N^2)$ where the function β' will be well-defined. If we add enhanced elliptic curves for $\Gamma_0(N)$ in maps (4.1), i.e. maps $(E,P) \to (E,\langle P\rangle)$ and $(E',P') \to (E',\langle P'\rangle)$, we obtain additional conditions on those preimages. Consequently, β' will belong to a smaller function field $k(X(\Gamma'))$, for some congruence subgroup Γ' satisfying $\widetilde{\Gamma}(N) \subset \Gamma'$. The groups that describe the preimages and their connections to the function fields are provided in the following lemma.

Lemma 4.1. *Let $N \geq 5$ be a positive integer. Group G, defined as a semidirect product*

$$G = (\mathbb{Z}/N\mathbb{Z})^2 \rtimes_{\widehat{\varphi}} (\mathbb{Z}/N\mathbb{Z})^\times,$$

where for a triple $((g_1,g_1'),g_2) \in G$ we have $\widehat{\varphi}_{g_2}(g_1,g_1') = (g_2g_1, g_2g_1')$, is isomorphic to Galois group of function field extension $k(X_1(N^2))/k(X_0(N))$. In particular $k(X_0(N)) = k(X_1(N^2))^G$. Let subgroup H of G be defined as

$$H = (\mathbb{Z}/N\mathbb{Z} \times \{0\}) \rtimes_{\widehat{\varphi}} (\mathbb{Z}/N\mathbb{Z})^\times,$$

and let $\pi_{1,N}, \pi_{2,N}, \psi_N$ be pullback operators defined by

$$\begin{aligned}
\pi_{1,N}^* &\colon k(X_1(N)) \to k(X_1(N^2)),\ \pi_{1,N}((E,R)) = (E,[N]R), \\
\pi_{2,N}^* &\colon k(X_1(N)) \to k(X_1(N^2)),\ \pi_{2,N}((E,R)) = (E/\langle [N]R\rangle, R+\langle [N]R\rangle), \\
\psi_N^* &\colon k(X_0(N)) \to k(X_1(N)),\ \psi_N((E,P)) = (E,\langle P\rangle).
\end{aligned}$$

Functions from the set $\pi_{1,N}^*(\psi_N^*(k(X_0(N))))$ are invariant under the action of group G and functions from the set $\pi_{2,N}^*(\psi_N^*(k(X_0(N))))$ are invariant under the action of subgroup H.

Proof. Let E be an elliptic curve over the field k and P a point of order N on that curve. Let R and R' be points of order N^2 on curve E and R such that $P = [N]R$. Pair (E, R) is an enhanced elliptic curve for $\Gamma_1(N^2)$. We are interested in preimages of composition $\pi_{1,N}^* \circ \psi_N^*$, i.e. in map $(E, R) \mapsto (E, \langle [N]R \rangle)$. Different R and R' are mapped to the same point if $\langle [N]R \rangle = \langle [N]R' \rangle$, so there exists $k \in \mathbb{N}$ such that $[kN]R = [N]R'$. Because R' is a point of order N^2 and $[k]P = [N]R'$ it follows that $\gcd(N, k) = 1$. Altogether, points

$$R' = [k]R + \overline{P}, \text{ where } \overline{P} \in E[N] \text{ and } k \in \mathbb{N}, \ \gcd(k, N) = 1,$$

are mapped by $(E, R) \mapsto (E, \langle [N]R \rangle)$ to the same final point. Number of preimages of this type is $N^2 \varphi(N)$.[4]

Define $G_1 := (\mathbb{Z}/N\mathbb{Z})^2$ and $G_2 := (\mathbb{Z}/N\mathbb{Z})^\times$. Let torsion group $E[N]$ be generated by the basis $\langle P_1, P_2 \rangle$, so a point $\overline{P} \in E[N]$ can be expressed as $\overline{P} = [a]P_1 + [b]P_2$ for some $a, b \in \mathbb{Z}/N\mathbb{Z}$. Point R' is equal to $[k]R + [a]P_1 + [b]P_2$. We define action of the triple $(a, b, k) \in G_1 \rtimes_{\widehat{\varphi}} G_2$ on the point R, i.e. on the set of preimages, with

$$(a, b, k)R \mapsto [k]R + [a]P_1 + [b]P_2. \tag{4.2}$$

This is a well-defined action, because for two such triples $(a_1, b_1, k_1), (a_2, b_2, k_2)$, we have:

$$\begin{aligned} (a_1, b_1, k_1) \circ (a_2, b_2, k_2)R &= (a_1, b_1, k_1)([k_2]R + [a_2]P_1 + [b_2]P_2) \\ &= [k_1]([k_2]R + [a_2]P_1 + [b_2]P_2) + [a_1]P_1 + [b_1]P_2 \\ &= [k_1k_2]R + [k_1a_2 + a_1]P_1 + [k_1b_2 + b_1]P_2 \\ &= (a_1 + k_1a_2, b_1 + k_1b_2, k_1k_2)R. \end{aligned}$$

Let $G = G_1 \rtimes_{\widehat{\varphi}} G_2$ and $\widehat{\varphi}_k(a, b) = (ka, kb)$, $a, b \in G_1, k \in G_2$. We have identified functions from $k(X_0(N))$ with their double pullbacks first by ψ_N and then by $\pi_{1,N}$. More generally, a function field $k(X_0(N))$ was identified with $\pi_{1,N}^*(\psi_N^*(k(X_0(N)))$. Set of preimages of functions in $\pi_{1,N}^*(\psi_N^*(k(X_0(N))))$ is invariant under the action (4.2) of group G which implies $k(X_0(N)) = k(X_1(N^2))^G$.

For H, we are interested in the preimages of composition $\pi_{2,N}^* \circ \psi_N^*$, i.e. in map $(E, R) \mapsto (E/\langle [N]R \rangle, \langle R + \langle [N]R \rangle \rangle)$. As before, for the condition $\langle [N]R \rangle = \langle [N]R' \rangle$ there exists $\hat{h} \in \mathbb{N}$, $\gcd(\hat{h}, N) = 1$ such that $R' = [\hat{h}]R + \overline{P}$, for some $\overline{P} \in E[N]$. When R and R' are satisfying this, second condition becomes $\langle R + \langle [N]R \rangle \rangle = \langle R' + \langle [N]R \rangle \rangle$, i.e. $\langle R + \langle P \rangle \rangle = \langle R' + \langle P \rangle \rangle$. Now, there exists $\hat{j}, \hat{s}$ such that $[\hat{j}]R - R' = [\hat{s}]P$. Combining everything together, $[\hat{j}]R - [\hat{h}]R - \overline{P} = [\hat{s}]P$, and $[\hat{j} - \hat{h}]R = [\hat{s}]P + \overline{P}$. Right side of this equality is a point of order dividing N, so $N | (\hat{j} - \hat{h})$ and there exist $\hat{t}$ such that $\hat{j} - \hat{h} = N\hat{t}$. Now, $[\hat{t}]P = [\hat{s}]P + \overline{P}$ meaning $\overline{P} \in \langle P \rangle$. Altogether, points of the form

$$R' = [h]R + \overline{P}, \text{ where } \overline{P} \in \langle P \rangle \text{ and } h \in \mathbb{N}, \ \gcd(h, N) = 1$$

are mapped by $(E, R) \mapsto (E/\langle [N]R \rangle, \langle R + \langle [N]R \rangle \rangle)$ to the same final point. Number of preimages of this type is $N\varphi(N)$. The difference here is that we are not working with the whole torsion group $E[N]$, but with subgroup generated by a point P of order N. Using a analogous calculation as for G, functions in $\pi_{2,N}^*(\psi_N^*(k(X_0(N))))$ are invariant under the action of subgroup $H = (\mathbb{Z}/N\mathbb{Z} \times \{0\}) \rtimes_{\widehat{\varphi}} (\mathbb{Z}/N\mathbb{Z})^\times$. □

Subgroup H from Lemma 4.1 can be used to define a function field $k' := k(X_1(N^2))^H$. Field k' is an intermediate field $k(X_0(N)) \subset k' \subset k(X_1(N^2))$ and a function field for some modular curve, so we can take $k' = k(X(\Gamma'))$, where Γ' is a congruence subgroup and $X(\Gamma') := \Gamma'/\mathcal{H}$. All functions from the set $\pi_{2,N}^*(\psi_N^*(k(X_0(N))))$ are well-defined on the quotient $X(\Gamma')$ due to their invariant property under the action of H. From the construction above, Γ' is a subset of

[4] Throughout the proof φ denotes Euler totient function.

$\Gamma_0(N)$ and from the calculated number of preimages, index $[\Gamma_0(N) : \Gamma'] = N$. The congruence subgroup Γ' can be calculated similarly to the congruence subgroup $\widetilde{\Gamma}(N)$ from the previous section.

Using the setup and the proof of Lemma 4.1 and the discussion above, we can prove the following theorem.

Theorem 4.2. *Let H be a group $(\mathbb{Z}/N\mathbb{Z} \times \{0\}) \rtimes_{\widehat{\varphi}} (\mathbb{Z}/N\mathbb{Z})^\times$. Let k' be a function field defined as $k' := k(X_1(N^2))^H$. Extension $k'/k(X_0(N))$ is not a Galois extension.*

Proof. Let group G and pullbacks $\pi_{1,N}, \pi_{2,N}, \psi_N$ be defined as in Lemma 4.1. As discussed above, k' is by definition an intermediate field $k(X_0(N)) \subset k' \subset k(X_1(N^2))$ and there exists a congruence subgroup Γ' such that $k' = k(X(\Gamma'))$. Working with function fields shown in Figure 3, to get radical isogeny formulas on $X_0(N)$, we need to find an $\alpha \in k(X_0(N))$ such that $k(X_0(N))(\sqrt[N]{\alpha}) = k(X(\Gamma'))$. Functions from $k(X_0(N))$ are identified with composition of pullbacks $\pi_{1,N}$ and ψ_N, i.e. α should be an element of the field $\pi_{1,N}^*(\psi_N^*(k(X_0(N))))$. If such α exists, field extension $k(X(\Gamma'))/k(X_0(N))$ should be a cyclic extension of order N, i.e. it should be a Galois extension. This implies that H, a subgroup of index N, should be a normal subgroup of G.

Points of type $R' = R + [l]P$, $l \in \mathbb{N}$ are mapped by $(E, R) \mapsto (E/\langle [N]R\rangle, R + \langle [N]R\rangle)$ to the same final point. Corresponding congruence subgroup describing preimages of this type was calculated in Proposition 3.1 and it is equal to

$$\widetilde{\Gamma}(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \colon c \equiv 0 \pmod{N^2},\ a, d \equiv 1 \pmod{N} \right\}.$$

The index $[\widetilde{\Gamma}(N) \colon \Gamma_1(N^2)]$ is equal to N. This, combined with the calculated number of preimages in the proof of Lemma 4.1, implies that $\widetilde{\Gamma}(N) \subset \Gamma'$ with index equal to $\varphi(N)$. Function β' is an element of $k(X(\widetilde{\Gamma}(N)))$ by definition and an element of $k(X(\Gamma'))$ by construction.

If H is a normal subgroup, then for every $g \in G$ and every $h \in H$ there should exist some $h' \in H$ such that $ghg^{-1} = h'$. Let $g = ((g_1, g_2), k_1) \in G$ and $h = ((h_1, 0), k_2) \in H$. Using g and h,

$$\begin{aligned} ghg^{-1} &= ((g_1, g_2), k_1)((h_1, 0), k_2)((g_1, g_2), k_1)^{-1} \\ &= ((g_1, g_2), k_1)((h_1, 0), k_2)(\widehat{\varphi}_{k_1^{-1}}((g_1, g_2)^{-1}), k_1^{-1}) \\ &= ((g_1, g_2)\widehat{\varphi}_{k_1}(h_1, 0), k_1k_2)(\widehat{\varphi}_{k_1^{-1}}(-g_1, -g_2), k_1^{-1}) \\ &= ((g_1 + k_1h_1, g_2 + k_1 \cdot 0), k_1k_2)((-k_1^{-1}g_1, -k_1^{-1}g_2), k_1^{-1}) \\ &= ((g_1 + k_1h_1 - k_2g_1, g_2 - k_2g_2), k_2). \end{aligned}$$

For this product to be in H, $g_2 - k_2g_2$ should be equal to 0, for every $k_2 \in (\mathbb{Z}/N\mathbb{Z})^\times$ and every $g_2 \in \mathbb{Z}/N\mathbb{Z}$. Let g_2 be a generator for $\mathbb{Z}/N\mathbb{Z}$, for example, take $g_2 = 1$. Then, for every $k_2 \in (\mathbb{Z}/N\mathbb{Z})^\times, k_2 \neq 1$ we have $k_2g_2 = k_2 \cdot 1 = k_2 \neq 1 = g_2$. To conclude, H is not a normal subgroup of G. □

Returning to Example 2.4, the existence of radical isogeny formulas on $S_0(5)$ depends on finding a parametrization of $S_0(5)$ for which the extension $\mathbb{Q}(\zeta_5)(\beta')/\mathbb{Q}(\zeta_5)(\beta)$ is Galois. However, Theorem 4.2 proves that a Galois extension is not possible in a more generalized setting of modular curves. As a direct consequence of that fact, we have the following corollary which is the main result of this article.

Corollary 4.3. *Let $N \geq 5$. Radical isogeny formulas on $S_0(N)$ are not possible.*

$$\begin{tikzcd}
k(X_0(N)) \arrow[r, phantom, "\overset{N}{\subset}"] \arrow[rr, bend right, dash, "G"'] & k(X(\Gamma')) \arrow[r, phantom, "\subset"] \arrow[r, bend left, dash, "H"] & k(X_1(N^2))
\end{tikzcd}$$

FIGURE 3. Function fields related to groups G and H

REFERENCES

[1] Daniel J Bernstein, Luca De Feo, Antonin Leroux, and Benjamin Smith. Faster computation of isogenies of large prime degree. *Open Book Series*, 4(1):39–55, 2020.

[2] Fouazou Lontouo Perez Broon, Thinh Dang, Emmanuel Fouotsa, and Dustin Moody. Isogenies on twisted Hessian curves. *Journal of mathematical cryptology*, 15(1):345–358, 2021.

[3] Wouter Castryck and Thomas Decru. An efficient key recovery attack on SIDH (preliminary version). *Cryptology ePrint Archive*, 2022.

[4] Wouter Castryck, Thomas Decru, Marc Houben, and Frederik Vercauteren. Horizontal racewalking using radical isogenies. In *Advances in Cryptology–ASIACRYPT 2022: 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5–9, 2022, Proceedings, Part II*, pages 67–96. Springer, 2023.

[5] Wouter Castryck, Thomas Decru, and Frederik Vercauteren. Radical isogenies. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 493–519. Springer, 2020.

[6] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: an efficient post-quantum commutative group action. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 395–427. Springer, 2018.

[7] Daniel Cervantes-Vázquez, Mathilde Chenu, Jesús-Javier Chi-Domínguez, Luca De Feo, Francisco Rodríguez-Henríquez, and Benjamin Smith. Stronger and faster side-channel protections for CSIDH. In *International Conference on Cryptology and Information Security in Latin America*, pages 173–193. Springer, 2019.

[8] Denis X Charles, Kristin E Lauter, and Eyal Z Goren. Cryptographic hash functions from expander graphs. *Journal of CRYPTOLOGY*, 22(1):93–113, 2009.

[9] Keith Conrad. Semidirect products of groups. `https://kconrad.math.uconn.edu/blurbs/grouptheory/semidirect-product.pdf`. [Online; accessed 13-July-2022].

[10] Gary Cornell, Joseph H Silverman, and Glenn Stevens. *Modular forms and Fermat's last theorem*. Springer Science & Business Media, 2013.

[11] Craig Costello and Huseyin Hisil. A simple and compact algorithm for SIDH with arbitrary degree isogenies. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 303–329. Springer, 2017.

[12] Jean-Marc Couveignes. Hard homogeneous spaces. *Cryptology ePrint Archive*, 2006.

[13] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. SQISign: compact post-quantum signatures from quaternions and isogenies. In *Advances in Cryptology–ASIACRYPT 2020: 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7–11, 2020, Proceedings, Part I 26*, pages 64–93. Springer, 2020.

[14] Luca De Feo, Antonin Leroux, and Benjamin Wesolowski. New algorithms for the Deuring correspondence: SQISign twice as fast. *Cryptology ePrint Archive*, 2022.

[15] Pierre Deligne and Michael Rapoport. Les schémas de modules de courbes elliptiques. In *Modular functions of one variable II*, pages 143–316. Springer, 1973.

[16] Fred Diamond and Jerry Shurman. A first course in modular forms. In *Graduate Texts in Mathematics*, volume 228. Springer, 2005.

[17] David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In *Post-Quantum Cryptography: 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29–December 2, 2011. Proceedings 4*, pages 19–34. Springer, 2011.

[18] Nicholas M Katz and Barry Mazur. Arithmetic moduli of elliptic curves. *Annals of mathematics studies*, (108):R9–514, 1985.

[19] Suhri Kim, Kisoon Yoon, Young-Ho Park, and Seokhie Hong. Optimized method for computing odd-degree isogenies on Edwards curves. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 273–292. Springer, 2019.

[20] Luciano Maino and Chloe Martindale. An attack on SIDH with arbitrary starting curve. *Cryptology ePrint Archive*, 2022.

[21] Hiroshi Onuki and Tomoki Moriya. Radical isogenies on Montgomery curves. In *IACR International Conference on Public-Key Cryptography*, pages 473–497. Springer, 2022.

[22] Damien Robert. Breaking SIDH in polynomial time. *Cryptology ePrint Archive*, 2022.

[23] Alexander Rostovtsev and Anton Stolbunov. Public-key cryptosystem based on isogenies. *Cryptology ePrint Archive*, 2006.

[24] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer, 2009.

[25] Marco Streng. Generators of the group of modular units for $\Gamma^1(N)$ over the rationals. *arXiv preprint arXiv:1503.08127v2*, 2019.

[26] Jacques Vélu. Isogénies entre courbes elliptiques. *CR Acad. Sci. Paris, Séries A*, 273:305–347, 1971.

[27] Michał Wroński. Application of Velusqrt algorithm to Huff's and general Huff's curves. Cryptology ePrint Archive, Paper 2021/073, 2021. `https://eprint.iacr.org/2021/073`.