RADICAL ISOGENIES AND MODULAR CURVES

VALENTINA PRIBANIĆ

ABSTRACT. This article explores the connection between radical isogenies and modular curves. Radical isogenies are formulas introduced by Castryck, Decru, and Vercauteren at Asiacrypt 2020, designed for the computation of chains of isogenies of fixed small degree N. An important advantage of radical isogeny formulas over other formulas with a similar purpose, is that there is no need to generate a point of order N that generates the kernel of the isogeny. Radical isogeny formulas were originally developed using elliptic curves in Tate normal form, while Onuki and Moriya have proposed radical isogenies formulas of degrees 3 and 4 on Montgomery curves. Furthermore, they 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 (using Tate normal form) to the language of modular curves. In addition, we solve an open problem introduced by Onuki and Moriya regarding radical isogeny formulas on $X_0(N)$.

CONTENTS

1. INTRODUCTION

Isogeny-based cryptographic protocols are considered to be good candidates for post-quantum cryptography as they are believed to be resistant to quantum computer attacks. The main advantages of isogeny-based cryptography, in comparison to other post-quantum protocols, are smaller key sizes and smaller ciphertext sizes. On the other hand, the main disadvantage of isogeny-based protocols has been the high computational cost of encryption and decryption. Computing isogenies of low degree in finite field is needed in protocols such as Charles, Goren and Lauter's hash function [CLG09], Couveignes, Rostovtsev, Stolbunov key exchange protocol [Cou06, RS06] or Castryck, Lange, Martindale, Panny, and Renes key exchange CSIDH [CLM+18]. An isogeny can be computed from the coordinates of the points in its kernel using Vélu's formulas [Vél71]. To enhance and accelerate isogeny computation, several different approaches or variants of Vélu's formulas have been considered. There are many variants of Vélu's formulas on different curve models such as Montgomery curves in [CH17], Edwards curves [CVCCD+19, KYPH19] or Hessian curves [BDFM21]. There is also an algorithm by Bernstein, De Feo, Leroux and Smith [BDFLS20] that reduces the cost of computation of

isogeny of degree N from $\mathcal{O}(N)$ to $\widetilde{\mathcal{O}}(\sqrt{N})$ and application of that algorithm to Huff's and general Huff's curves in [Wro21].

Radical isogenies are formulas designed for the computation of a chain of isogenies of the same small degree between elliptic curves over finite field, first introduced by Castryck, Decru and Vercauteren in [CDV20]. They showed that using radical isogeny formulas in CSIDH-512 leads to more efficient implementation and a speed-up of 19%, see [CDV20, Section 6]. Elliptic curve E over the field k and a point $P \in k(E)$ of order $N \geq 4$ are, as a pair, isomorphic to the unique curve-point pair (notation remains the same) of form

$$E\colon y^2 + (1-c)xy - by = x^3 - bx^2,\ P = (0,0), \tag{1.1}$$

where $b, c \in k$. Pair (1.1) is said to be in Tate normal form. Using Vélu's formulas one can compute an isogeny $\varphi\colon E \to E'$ where $E' = E/\langle P\rangle$. Radical isogeny formulas are generating points P' on E' for which the composition $E \to E' \to E'/\langle P'\rangle$ is a cyclic isogeny of order N^2. Points P' (of order N) on E' can be defined as preimage of point P under the dual isogeny $\widehat{\varphi}\colon E' \to E$. Central observation for radical isogeny formulas is that the points P' are defined over field $k(b, c, \sqrt[N]{\rho})$, for some $\rho \in k(b, c)$. Coordinates of P' are explicitly calculated using formulas depending on b, c and $\sqrt[N]{\rho}$. Continuing from the curve E', this curve together with a point P' will also be isomorphic to a curve in Tate's normal form, now specified with coefficients b' and c'. Formulas derived in [CDV20, Section 3] express coefficients b' and c' as elements of $k(b, c, \sqrt[N]{\rho})$. Radical isogeny formulas can be repeated on this new curve, i.e. described process can be repeated iteratively, which results in a chain of isogenies of degree N.

Following [CSS13, Chapter III, Section 1.3] and [DS05, Section 1.5], enhanced elliptic curve for congruence subgroup

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

is defined as an ordered pair (E, P), where E is an elliptic curve over some algebraically closed field and P is a point of order N on that curve. Two enhanced elliptic curves for $\Gamma_1(N)$, (E, P) and (E', P') will be equivalent (denoted by $\sim$) if there is an isomorphism $E \to E'$ that takes P to P'. The corresponding set of equivalence classes is

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

Similar set $S_0(N)$, using elliptic curve and cyclic group of order N, can be defined for congruence subgroup $\Gamma_0(N)$. In Section 3 of this article, we will extend the notion of the radical isogeny formulas to modular functions. We will show that the parameters b and c, from Tate's normal form, can be used to define functions on the set of enhanced elliptic curves for $\Gamma_1(N)$. Furthermore, there is a function on the set of enhanced elliptic curves for $\Gamma_1(N^2)$ that acts as an equivalent to $\sqrt[N]{\rho}$ of the radical isogeny formulas.

In [OM22], Onuki and Moriya proposed radical isogeny formulas on Montgomery curves of degrees 3 and 4. Montgomery curve over field k is an elliptic curve

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

where $A \in k$ and $A^2 \neq 4$. Coefficient A determines a class of $(E, (0,0))$ in $S_0(4)$, see [OM22, 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 $N = 3, 4$, equality $S_0(N) = S_1(N)$ holds and the existence of radical isogeny formulas on $S_1(3), S_1(4)$ implies a radical isogeny formula on $S_0(3), S_0(4)$, i.e. there is a formula between Montgomery coefficients of curves, see [OM22, Section 3]. Methods used in [OM22] for cases $N = 3, 4$ cannot be directly extended to case $N \geq 5$ partly because $S_0(N) \neq S_1(N)$. The following example illustrates the reason why radical isogeny formulas for $S_0(N)$ when $N \geq 5$ are maybe not possible.

Example 1.1 ([OM22, Section 4])**.** Let $N = 5$. Let k be a field with $\mathrm{char}(k) \nmid N$ 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. 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 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 $\mathrm{Gal}(\mathbb{Q}(\zeta_5)(b')/\mathbb{Q}(\zeta_5)(\beta))$ 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 $\mathrm{Gal}(\mathbb{Q}(\zeta_5)(b')/\mathbb{Q}(\zeta_5)(\beta))$, thus extension $\mathbb{Q}(\zeta_5)(\beta')/\mathbb{Q}(\zeta_5)(\beta)$ cannot be a Galois extension.

If the parameter β' from Example 1.1 could be expressed as a rational expression depending on the parameter β, we would have a direct way to calculate b' with simpler formulas (quadratic equation) than the radical isogeny formulas. Because extension $\mathbb{Q}(\zeta_5)(\beta')/\mathbb{Q}(\zeta_5)(\beta)$ is not a Galois extension, this is not possible. Still, maybe it is 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. Finding such parametrization was left as an open problem in [OM22], and that open problem is solved in this article. We will show, using the generalization of radical isogeny formulas for the set of functions on enhanced elliptic curves for $\Gamma_0(N)$, in the Theorem 4.2, that such Galois extension could not exists. A straightforward consequence will be the following corollary.

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

Paper organization

Section 2 provides necessary background including brief overview on elliptic curves, isogenies of elliptic curves, definition of congruence subgroups, modular curves, semidirect product of groups and radical isogenies. Section 3 translates radical isogenies to the language modular curves. Section 4 extends the setting from Section 3 so that it includes modular curves on $X_0(N)$ and provides the proof to the Theorem 4.2 that, as a consequence, has a corollary that is a solution to the open problem described in Example 1.1.

2. Preliminaries

This section will provide summary of necessary background. For more details on elliptic and modular curves refer to [Sil09], [DS05] and [CSS13, Chapter III].

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

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 [Str19, Lemma 2.1].

If $\mathrm{char}(k) \nmid N$ we can define Tate pairing, 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 $E(k)[N]$ are all the points in $E[N]$ defined over k.

Following [Sil09, Chapter II.3], divisor for a curve E is defined as formal sum $\sum_{P\in E} n_P(P)$, where $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many $P \in E$. Miller function f_{N,P_1} is a function on E with divisor $N(P_1) - N(\mathcal{O}_E)$. Support for 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 $\{P_1, \mathcal{O}_E\}$. Support of this divisor is disjoint from 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, 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, 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

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

Function $g_{N,P}$ can be used to define Weil pairing, see [Sil09, 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 $\varphi(\mathcal{O}_E) = \mathcal{O}_{E'}$. Multiplication with N is an example of an isogeny. Except for the zero isogeny, every other isogeny is a finite map of curves so that 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 $\overline{k}(E)/\varphi^*(\overline{k}(E'))$. Isogeny is separable (inseparable, purely inseparable) if this finite extension is separable (inseparable, purely inseparable). For every isogeny φ there exists a dual isogeny $\widehat{\varphi}\colon E' \to E$ such that $\widehat{\varphi}\circ\varphi = [\deg(\varphi)]$. The kernel of isogeny is a finite subgroup of $E(\overline{k})$. The size of the kernel divides the degree of the isogeny and they are the same 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 [CDV20, 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

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

Principle congruence subgroup for $N > 0$ is

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

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

For an upper half plane $\mathcal{H} = \{\tau \in \mathbb{C}\colon \mathrm{Im}(\tau) > 0\}$ and matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbb{Z})$, the action on $z \in \mathcal{H}$ is defined as

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

Using this fractional linear transformation, for a congruence subgroup Γ, modular curve can be defined with

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

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. Enhanced elliptic curve for $\Gamma_0(N)$ is defined as ordered pair (E, C), where C is a cyclic subgroup of order N. Two enhanced elliptic curves $(E, C), (E', C')$ are equivalent if there exists some isomorphism $E \xrightarrow{\sim} E'$ that takes C to C'. Set of equivalence classes is

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

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 some isomorphism $E \xrightarrow{\sim} E'$ that takes P to P'. Set of equivalence classes is

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

Following [DS05, Chapter 1.3], complex elliptic curve E_τ can be defined as a quotient of the complex plane by the lattice

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

where $\Lambda_\tau = \mathbb{Z} \oplus \tau\mathbb{Z}$. Sets $S_0(N)$ and $S_1(N)$ are defined the same 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 construct a bijective map, to $\tau \in \mathcal{H}$, associate the pair $(E_\tau, \frac{1}{N} + \Lambda_\tau)$. Any pair (E, P) will be 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 [DS05, Theorem 1.5.1.]. □

Similar statements to the one in the Theorem 2.2 are true for congruence subgroups $\Gamma_0(N)$ and $\Gamma(N)$.

2.4. **Semidirect product of groups.** Following [Con], 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 [CDV20], this section will provide a necessary background for radical isogenies. Let k be a field, $N > 0$ such that $\mathrm{char}(k) \nmid N$, E elliptic curve over the field k and $P \in E(k)$ point of order N. Using Lemma 2.1, curve-point pair (E, P) is isomorphic to unique pair of 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 kernel $\langle P\rangle$. Let E' denote the model for $E/\langle P\rangle$ defined over k and P' point on E' of order N such that $\widehat{\varphi}(P') = P$, where $\widehat{\varphi}$ is a dual isogeny of φ. Point P' satisfying this condition is called P-distinguished. This point is not unique. From [CDV20, Theorem 5] for coordinates of the point P' there exists a formula depending on b, c and $\sqrt[N]{\rho}$, where ρ is representative of Tate pairing $t_N(P, -P)$, i.e. point P' is defined over $k(b, c, \sqrt[N]{\rho})$. As P' is of order N on curve E', there is a Tate normal form for this pair defined with the unique coefficients b', c'. The iterative process of radical isogeny formulas can be repeated on pair (E', P'). Additionally, formulas for b' and c' can be expressed directly as elements of the field extension $k(b, c, \sqrt[N]{\rho})$. This field extension is a simple radical extension. Field extension $k \subset L$ is simple radical extension of degree $N \geq 2$ if there exists α such that $L = k(\alpha), \alpha^N \in k$ and $x^N - \alpha^N \in k[x]$ is irreducible. Explicit radical isogeny formulas when $N = 5$, are written in the following example:

Example 2.3 ([CDV20, Section 4])**.** Let $N = 5$. Elliptic curve E has 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

$$\begin{aligned} x_0' &= 5\alpha^4 + (b-3)\alpha^3 + (b+2)\alpha^2 + (2b-1)\alpha - 2b, \\ y_0' &= 5\alpha^4 + (b-3)\alpha^3 + (b^2 - 10b + 1)\alpha^2 + (13b - b^2)\alpha - b^2 - 11b. \end{aligned}$$

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

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

and the process can be repeated.

The usual method of calculating isogenies requires a point of a specific order for every isogeny in the chain of isogenies that is calculated. With radical isogeny formulas, having a point of a specific order is only necessary for the first step, i.e. the one step that uses Vélu's formulas. Calculating isogenies in consecutive steps of the process does not depend on knowledge of any torsion point. The list of formulas for radicand ρ for $N \leq 13$ can be found in [CDV20, Section 5].

3. Radical isogenies in the language of modular curves

Let E be an elliptic curve over the field k where $\mathrm{char}(k) \nmid N$ and P point of order $N \geq 4$ on that curve. From Lemma 2.1, pair (E, P) is isomorphic to the unique pair of the form

$$E\colon y^2 + (1-c)xy - by = x^3 - bx^2,\ P = (0,0),\ b, c \in k.$$

Let φ be an isogeny $E \to E/\langle P\rangle$ with $\mathrm{Ker}(\varphi) = \langle P\rangle$. Define $E' \coloneqq E/\langle P\rangle$. There is a point $P' \in E'$ of order N such that $\widehat{\varphi}(P') = P$. Point P' is not unique $P-$distinguished point such that composition $E \to E' \to E'/\langle P'\rangle$ is a cyclic N^2 isogeny. Again, using Lemma 2.1, pair (E', P') is isomorphic to unique pair of the form

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

It follows from [CDV20, Section 3] that the point P', parameters b', c' are all defined over $k(b, c, \sqrt[N]{\rho})$ for some $\rho \in k(b, c)$. 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 $\Gamma_1(N)$, that for a curve $(\widetilde{E}, \widetilde{P})$ returns parameter $\widetilde{b}$ from corresponding Tate normal form. This is a well-defined function because Tate's normal form is unique. Similar, 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. 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 point P' is not unique, the map $(E, P) \to (E', P')$ is not uniquely defined, so there is none obvious connection on $X_1(N)$. For a point P of order N, let R be a point of order N^2 such that $NR = P$. Point R is not unique. Pair (E, R) is an enhanced elliptic curve for $\Gamma_1(N^2)$, and starting from (E, R), we can go in two directions. The first one on E, knowing that there is a point $P = NR$, and the second on E', using P and R, we can define a point P' on $E/\langle NR\rangle$ of order N as

$$P' \coloneqq R + \langle NR\rangle = R + \langle P\rangle.$$

From $\varphi(R) = P'$ we have

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

so P' is $P-$distinguished. After the introduction of point R, the sequence of maps (3.1) can be slightly modified. For simplicity, we will continue to work with parameter b and associated functions, as the approach for c is the same. Starting from the enhanced elliptic curve (E, R), maps are

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

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

From the maps in (3.3), similar to $\mathbf{b}$, we can 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.

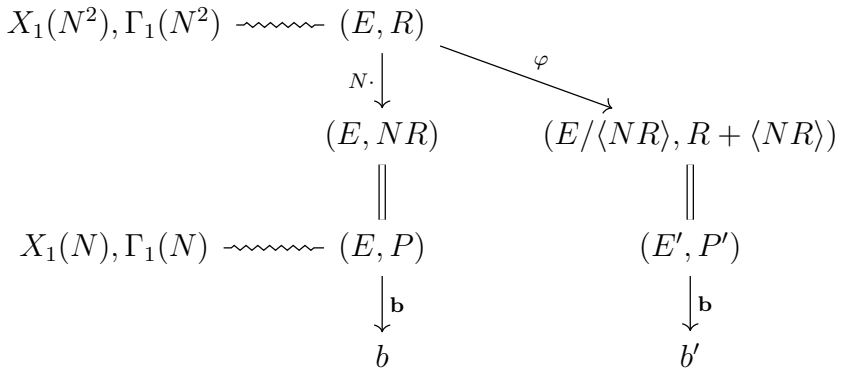

FIGURE 1. Maps on enhanced elliptic curves

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:

$$\pi_{1,N}^*\colon k(X_1(N))\to k(X_1(N^2)),\ \pi_{1,N}((E,R))=(E,NR),$$
$$\pi_{2,N}^*\colon k(X_1(N))\to k(X_1(N^2)),\ \pi_{2,N}((E,R))=(E/\langle NR\rangle, R+\langle NR\rangle).$$

From

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

and

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

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

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

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 $f_{N,P}$ normalized Miller function. With the value of $f_{N,P}$ in point $-P$, we can define a modular function f on enhanced elliptic curves for $\Gamma_1(N)$,

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

For a Miller function $f_{N,P}$ and point P, defined as above, 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 enhanced elliptic curve (E,R), where, as before, $P=NR$, we have a function on $X_1(N^2)$,

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

Function $g\coloneqq(E,R)\mapsto g_{N,P}(-R)\in k(X_1(N^2))$ is a function with property

$$g^N=f,$$

so $N-$th root of f is a function on $X_1(N^2)$. To summarize, functions b, b' and g are elements of $k(X_1(N^2))$, but due to the size of this field, proving (3.4) is still not possible, and it is necessary to find a smaller quotient of $X_1(N^2)$ where b, b', and g are well defined.

3.1. **"Shrinking" the field of definition.** To get a better sense of the behaviour of the function b', preimages of (E, P) under the pullback operator $\pi_{2,N}$, i.e. pairs (E, R) and (E, R'), mapped by $\pi_{2,N}$ to the same point $(E/\langle NR\rangle, R + \langle NR\rangle)$ will be investigated. For equality

$$(E/\langle NR'\rangle, R' + \langle NR'\rangle) = (E/\langle NR\rangle, R + \langle NR\rangle)$$

to be true we need to have $\langle NR'\rangle = \langle NR\rangle$ and $R' + \langle NR'\rangle = R + \langle NR\rangle$. Combined, $R' + \langle NR\rangle = R + \langle NR\rangle$, so there exists some $l \in \mathbb{N}$ such that,

$$R' = R + l \cdot NR \text{ and } NR' = N(R + lP)$$

thus altogether,

$$\langle N(R + lP)\rangle = \langle NR\rangle.$$

Considering that point R is of order N^2, points $(E, R), (E, R+1\cdot NR), \ldots, (E, R+(N-1)\cdot NR)$ are all mapped to the same final point. Comparing this to the definition of b', it is clear that b' is a function on $X_1(N^2)$ that maps points of this type to the same final point.

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

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

Order of operator t is equal to N, because we have $t^N(E, R) = (E, (N+1)^N R) = (E, R)$. The definition of operator t mimics the mapping on points from the beginning of this section. From the composition of t with $\pi_{1,N}$ on enhanced elliptic curve (E, R) we have

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

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

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

thus, every pullback by $\pi_{2,N}$ or by $\pi_{1,N}$ will be invariant for t. Modular function $(E, R) \overset{g}{\mapsto} g_{N,P}(-R)$, with property $g^N = f$, is also invariant for t. Referring again to [Sil09, Chapter III.8] for more details, function $g_{N,NR}$ can be used to define Weil pairing

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

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

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

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

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

Group of automorphisms of $X_1(N^2)$ generated with t will be denoted with $\langle t\rangle$. Function on $X_1(N^2)$, invariant for the operator t, can be viewed as a function on a quotient $X_1(N^2)/\langle t\rangle$. From the discussion above, b' is an example of a function on $X_1(N^2)/\langle t\rangle$. Quotient $X_1(N^2)/\langle t\rangle$, i.e. quotient of modular curve with the operator is again a modular curve. To see this, following [KM85] and [DR73] we can, for a field k defined at the begging of this section, assume 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 automorphism of $X_1(N^2)$ generated with t. Quotient of the $\mathcal{H}^*=\mathcal{H}\cup\mathbb{Q}\cup\{\infty\}$ and the congruence subgroup

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

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

Proof. Following [DS05, 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 invariant for $\Gamma_1(N^2)$ and matrix $\mathbf{t}\in\mathrm{SL}_2(\mathbb{Z})$, which corresponds to the operator t. To see this, first notice that from the Theorem 2.2, $S_1(N^2)$ 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 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'. For 1 is obvious 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. Now is easy to see that 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 with $\Gamma_1(N^2)$ and matrix $\mathbf{t}$, thus

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

It is obvious from the construction of the congruence subgroup $\widetilde{\Gamma}(N)$ that the quotient $\widetilde{\Gamma}(N)/\mathcal{H}^*$ is defining a modular curve consisting of all functions on $X_1(N^2)$ invariant for 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

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

Subgroup $\Gamma_1(N^2)$ 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 $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(N^2)$ and $\mathbf{t}$ as in proof of the Proposition 3.1, which is true because

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

For the index of $\Gamma_1(N^2)$ in $\widetilde{\Gamma}(N)$, we will use homomorphism $\pi_N\colon \mathrm{SL}(\mathbb{Z}) \to \mathrm{SL}(\mathbb{Z}/N\mathbb{Z})$, induced by reduction modulo N, where $N \geq 1$. The principle congruence subgroup $\Gamma(N)$ is the kernel of this homomorphism and a normal subgroup in $\mathrm{SL}(\mathbb{Z})$ of finite index. Any other congruence subgroup $\Gamma(N) \subset \widetilde{\Gamma}$ is of finite index in $\mathrm{SL}(\mathbb{Z})$ and a preimage of π_N, i.e. $\widetilde{\Gamma} = \pi_N^{-1}(\widehat{\Gamma})$ where $\widehat{\Gamma}$ is some subgroup of $\mathrm{SL}(\mathbb{Z}/N\mathbb{Z})$. Index $[\widetilde{\Gamma}\colon \Gamma(N)]$ is equal to $\#\widehat{\Gamma}$. In our case for $\#\widehat{\widetilde{\Gamma}(N)}$, after reducing elements of $\widetilde{\Gamma}(N)$ modulo N^2, 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 element b, but a and d have to satisfy a condition for determinant $ad \equiv 1 \pmod{N^2}$. If we write $a = 1 + kN$ and $d = 1 + lN$, where $k, l \in \{0, 1, \ldots, N-1\}$, then

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

from which $k + l \equiv 0 \pmod{N}$, so l depends completely on k meaning d depends completely on a. Altogether, $\#\widehat{\widetilde{\Gamma}(N)} = N^3$. 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

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

With similar calculation, index $[\Gamma_1(N)\colon \Gamma_1(N^2)]$ is equal to N^2.

Subgroup $\Gamma_1(N^2)$ is a normal subgroup of $\widetilde{\Gamma}(N)$ with the index N, so 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.

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

from which

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

so we have an equality of function fields

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

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

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

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

Lemma 3.2. *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 $P = NR$ 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 with $t(E, R) = (E, (N+1)R)$, $(E, R) \in S_1(N^2)$. Let $\pi_{1,N}^*\colon k(X_1(N)) \to k(X_1(N^2)$ be a pullback operator defined with $\pi_{1,N}((E, R)) = (E, NR)$. Then the polynomial $x^N - f$ is irreducible polynomial in $\pi_{1,N}^*(k(X_1(N)))[x]$.*

Proof. We will show that field extension $\pi_{1,N}^*(k(X_1(N)))(g)$ is of degree N over $k(X_1(N))$, i.e. that the function g is only invariant for the operator t, so 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 $\widetilde{\Gamma}(N) \subsetneq \Gamma \subset \Gamma_1(N)$ and $g \in k(X(\Gamma))$.

Assume then that g is invariant for 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 $NT(R) = NR = P$. Invariant property of function g, together with previously defined Weil pairing implies:

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

Point $R - T(R)$ is in $E[N]$, because from the assumption $NT(R) = NR = P$, we have $N(R - T(R)) = P - P = \mathcal{O}$, so $e_N(P, R-T(R))$ is consistent with the definition of Weil pairing. From this, for every $(E,R) \in S_1(N^2)$ we have $e_N(P, R - T(R)) = 1$.
For a fixed elliptic curve E and P point of order N on that curve such that $P = NR$, as Weil pairing is non-degenerate, from $e_N(P, R - T(R)) = 1$, for every R, we have that the point $R - T(R) \in \langle P \rangle$. Point $T(R)$ then has a form $R + lP$ for some $l \in \mathbb{Z}$, depending on R.

Comparing this to the operator t, since g is invariant to t, we have

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

so $g(E,R) = g(E, R + kP)$ for every $k \in \mathbb{Z}$. For the operator T, we have

$$g(E,R) = g(E, T(R)) = g(E, R + lP),$$

for some $l \in \mathbb{Z}$, thus the invariant property of the function g for the operator T follows from the invariant property of the function g for the operator t, so g is modular only for the congruence subgroup $\widetilde{\Gamma}(N)$.

This implies that function field $\pi_{1,N}^*(k(X_1(N)))(g)$ is a extension of degree exactly N over $k(X_1(N))$. Roots of the polynomial $x^N - f$ are of the form $\zeta_N^k g$, where ζ_N is $N-$th root of unity and $k \in \mathbb{N}$. If we assume that this polynomial is not irreducible, then there would exists two non-constant polynomials $f_1, f_2 \in k(X_1(N))[x]$, such that $x^N - f = f_1(x) f_2(x)$, where $deg\ f_1 < N$ and g a root for f_1 which is a contradiction with the degree of g. □

To conclude, irreducibility of the polynomial $x^N - f$ from the Lemma 3.2 implies

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

meaning b' is element of $\pi_{1,N}^*(k(X_1(N)))(g)$, so equality (3.4) holds and radical isogeny formulas can be extended to modular functions.

Example 3.3. Let $N = 5$ and E be an elliptic curve over the field

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

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, guaranties that 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 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 [Str19].

In case of $N = 5$ we have $F_5(b, c) = b - c = 0$ and this implies a simpler Tate normal form (3.5). On the other side curve E' and point P' of order 5 are

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

Having only a parameter b results in only a modular function $\mathbf{b}$ in $k(X_1(5))$. For a point P, let R be a point of order 25 such that $5R = P$. Pair (E, R) is enhanced elliptic curve for $\Gamma_1(25)$. Pullbacks $\pi_{1,5}, \pi_{2,5}$ and maps b, b' are defined as before.

From the example in [CDV20, 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 $(E, R) \overset{g}{\mapsto} g_{5,5R}(-R)$ is a well defined map with a property $g^5 = b$.

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

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

Functions b', g and every pullback by $\pi_{1,5}$ or $\pi_{1,5}$ are invariant for 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 $\tilde{c} = 0, \tilde{a}, \tilde{d} \equiv 1 \pmod 5$ and $\tilde{a}, \tilde{b}, \tilde{c}, \tilde{d} \in \mathbb{Z}/25\mathbb{Z}$. Only possibilities for $\tilde{a}$ and $\tilde{d}$ are from set $\{1, 6, 11, 16, 21\}$. Determinant of the matrix has to be 1 in $\mathrm{SL}(\mathbb{Z}/25\mathbb{Z})$, there are 25 possibilities for $\tilde{b}$, so altogether, there are 125 elements in this group. Therefore, index $[\widetilde{\Gamma}(5) \colon \Gamma_1(25)] = 5$. Field extension $\pi_{1,5}^*(k(X_1(5))) \subset k(X_1(25)/\langle t\rangle)$ is of order 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 expanded 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 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 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 function $\boldsymbol{\beta}$ with $\beta \coloneqq \pi_{1,N}^*(\psi_N^*(\boldsymbol{\beta}))$ and define $\beta' \coloneqq \pi_{2,N}^*(\psi_N^*(\boldsymbol{\beta}))$. 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 for the operator t which implies $\beta' \in k(X(\widetilde{\Gamma}(N)))$. Similar to the previous section, if radical isogeny formulas exists 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 $(E, \langle NR\rangle)$ and $(E/\langle NR\rangle, \langle R + \langle NR\rangle\rangle)$. Moreover, to include functions on

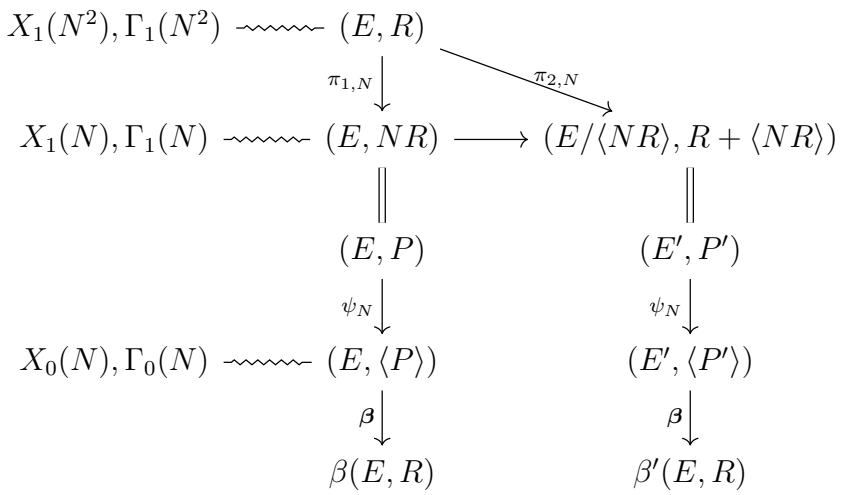

FIGURE 2. Maps on enhanced elliptic curves, including $X_0(N)$

$X_0(N)$, maps (3.2) and (3.3) are extended to

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

Describing preimages of maps in (4.1) will provide us with another quotient of $X_1(N^2)$ where function β' will be well defined. Addition of enhanced elliptic curves for $\Gamma_0(N)$ in maps (4.1), i.e. maps $(E,P) \to (E,\langle P\rangle)$ and $(E',P') \to (E',\langle P'\rangle)$ results in additional conditions on those preimages and, as a consequence, β' will be an element of a smaller function field $k(X(\Gamma'))$, for some congruence subgroup Γ' such that $\widetilde{\Gamma}(N) \subset \Gamma'$. Groups describing preimages and their connections to the function fields are given in the following proposition.

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

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

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 point of order N on that curve. Let R and R' be points of order N^2 on curve E and R such that $P = NR$. 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 $(E,R) \mapsto (E,\langle NR\rangle)$. Different R and R' are mapped to the same point if $\langle NR\rangle = \langle NR'\rangle$, so there exists $k \in \mathbb{N}$ such that $kNR = NR'$. Because R' is a point of order N^2 and $kP = NR'$ it follows that $\gcd(N,k) = 1$. Altogether, points

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

are mapped by $(E,R)\mapsto(E,\langle NR\rangle)$ to the same final point. Number of preimages of this type is $N^2\varphi(N)$.[1]
Define $G_1 \coloneqq (\mathbb{Z}/N\mathbb{Z})^2$ and $G_2 \coloneqq (\mathbb{Z}/N\mathbb{Z})^\times$. Let torsion group $E[N]$ be generated with basis $\langle P_1,P_2\rangle$, then a point $\overline{P}\in E[N]$ is equal to $\overline{P}=aP_1+bP_2$ for some $a,b\in\mathbb{Z}/N\mathbb{Z}$. Point R' is equal to $kR+aP_1+bP_2$. We define action of the triple $(a,b,k)\in G_1\rtimes_\varphi G_2$ on the point R, i.e. on the set of preimages, with

$$(a,b,k)R\mapsto kR+aP_1+bP_2. \tag{4.2}$$

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:

$$\begin{aligned}(a_1,b_1,k_1)\circ(a_2,b_2,k_2)R &= (a_1,b_1,k_1)(k_2R+a_2P_1+b_2P_2)\\ &= k_1(k_2R+a_2P_1+b_2P_2)+a_1P_1+b_1P_2\\ &= k_1k_2R+(k_1a_2+a_1)P_1+(k_1b_2+b_1)P_2\\ &= (a_1+k_1a_2,b_1+k_1b_2,k_1k_2)R.\end{aligned}$$

Let $G=G_1\rtimes_\varphi G_2$ 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 preimages of composition $\pi_{2,N}^*\circ\psi_N^*$, i.e. in map $(E,R)\mapsto(E/\langle NR\rangle,\langle R+\langle NR\rangle\rangle)$. Similar as before for condition $\langle NR\rangle=\langle NR'\rangle$ 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 $\langle R+\langle NR\rangle\rangle=\langle R'+\langle NR\rangle\rangle$, 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

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

are mapped by $(E,R)\mapsto(E/\langle NR\rangle,\langle R+\langle NR\rangle\rangle)$ 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 group generated with point P of order N. With a similar 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 $k'\coloneqq k(X_1(N^2))^H$. 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 $X(\Gamma')\coloneqq\Gamma'/\mathcal{H}$. Invariant property of the functions in the set $\pi_{2,N}^*(\psi_N^*(k(X_0(N))))$ under the action of H implies that all functions from that set are well defined on the quotient $X(\Gamma')$. From the construction above, Γ' is a subset of $\Gamma_0(N)$ 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 proof of the 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 with $k'\coloneqq k(X_1(N^2))^H$. Extension $k'/k(X_0(N))$ is not a Galois extension.*

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

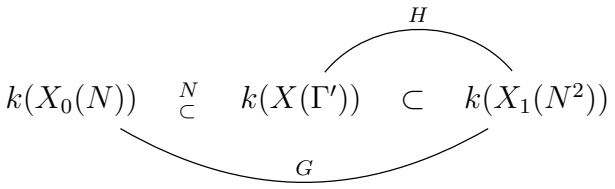

FIGURE 3. Function fields related to groups G and H

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 exist 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 $\alpha \in k(X_0(N))$ 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 $R' = R + lP,\ l \in \mathbb{N}$ are mapped by $(E, R) \mapsto (E/\langle NR\rangle, R + \langle NR\rangle)$ to the same final point. Corresponding congruence subgroup describing preimages of this type was calculated in Proposition 3.1 and it is equal to

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

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 the 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,

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

For this product to be in H, $g_2 - k_2 g_2 = 0$, 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 $k_2 g_2 = k_2 \cdot 1 = k_2 \neq 1 = g_2$. To conclude, H is not a normal subgroup of G. □

Coming back to Example 1.1, existence of radical isogeny formula for $S_0(5)$ depends on finding a parametrization of $S_0(5)$ for which the extension $\mathbb{Q}(\zeta_5)(\beta')/\mathbb{Q}(\zeta_5)(\beta)$ would be Galois. The Theorem 4.2 shows that such Galois extension cannot exists in a more generalized setting of modular curves. As a direct consequence of that fact, we have the following corollary which is a main result of this article.

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

REFERENCES

[BDFLS20] 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.

[BDFM21] 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.

[CDV20] 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.

[CH17] 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.

[CLG09] Denis X Charles, Kristin E Lauter, and Eyal Z Goren. Cryptographic hash functions from expander graphs. *Journal of CRYPTOLOGY*, 22(1):93–113, 2009.

[CLM+18] 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.

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

[Cou06] Jean-Marc Couveignes. Hard homogeneous spaces. *Cryptology ePrint Archive*, 2006.

[CSS13] Gary Cornell, Joseph H Silverman, and Glenn Stevens. *Modular forms and Fermat's last theorem*. Springer Science & Business Media, 2013.

[CVCCD+19] 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.

[DR73] Pierre Deligne and Michael Rapoport. Les schémas de modules de courbes elliptiques. In *Modular functions of one variable II*, pages 143–316. Springer, 1973.

[DS05] Fred Diamond and Jerry Shurman. A first course in modular forms. In *Graduate Texts in Mathematics*, volume 228. Springer, 2005.

[KM85] Nicholas M Katz and Barry Mazur. Arithmetic moduli of elliptic curves. *Annals of mathematics studies*, (108):R9–514, 1985.

[KYPH19] 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.

[OM22] Hiroshi Onuki and Tomoki Moriya. Radical isogenies on Montgomery curves. In *IACR International Conference on Public-Key Cryptography*, pages 473–497. Springer, 2022.

[RS06] Alexander Rostovtsev and Anton Stolbunov. Public-key cryptosystem based on isogenies. *Cryptology ePrint Archive*, 2006.

[Sil09] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer, 2009.

[Str19] Marco Streng. Generators of the group of modular units for $\Gamma^1(N)$ over the rationals. *arXiv preprint arXiv:1503.08127v2*, 2019.

[Vél71] Jacques Vélu. Isogénies entre courbes elliptiques. *CR Acad. Sci. Paris, Séries A*, 273:305–347, 1971.

[Wro21] 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`.

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

Email address: `valentina.pribanic@gmail.com`