ON SOME NON-LINEAR RECURRENCES OVER FINITE FIELDS LINKED TO ISOGENY GRAPHS

JUAN JESÚS LEÓN AND VICENTE MUÑOZ

Abstract. This paper presents new results that establish connections between isogeny graphs and nonlinear recurrences over finite fields. Specifically, we prove several theorems that link these two areas, offering deeper insights into the structure of isogeny graphs and their relationship with nonlinear recurrence sequences. We further provide two related conjectures which may be worth of further research. These findings contribute to a better understanding of the endomorphism ring of a curve, advancing progress toward the resolution of the Endomorphism Ring Problem, which aims to provide a computational characterization of the endomorphism ring of a supersingular elliptic curve.

1. Introduction

1.1. **On the role of Isogenies in Cryptography.** Isogenies have become a fundamental object of study in the area of post-quantum cryptography. Also, their role in "traditional" cryptography through the years has been notable, as they are used in algorithms for point counting on elliptic curves and are furthermore behind many cryptographic developments (computing distortion maps for pairing-based cryptography, designing hash-functions, etc.). Thus, understanding isogenies, related objects and algorithms is crucial for tackling problems in many areas of modern cryptography (see, for instance, the recent surveys [4, 16]).

In a nutshell, an *isogeny* is a map connecting two algebraic curves which is surjective and preserves the underlying group structure (for precise definitions, see [18]). Two curves connected through an isogeny are said to be *isogenous*. Given two isogenous elliptic curves over a finite field, computing an isogeny between them is assumed to be a very hard computational problem (even if quantum resources are at hand); this problem is typically referred to as the *Isogeny Path Problem*. Proving that two such curves are isogenous is however possible in (classical) polynomial time, as Tate's isogeny theorem states that two elliptic curves over a finite field K are isogenous if and only if they have the same number of points over K. A very interesting problem motivated by practical

applications is finding ways to prove *knowledge* of an isogeny between two curves without actually revealing it [4].

Furthermore, in cryptography, we often consider classes of isogenous curves which are identified using special labels called j-invariants. In particular, if we work in a finite field $\mathbb{F}_{p^2}$ (for p prime and under certain conditions), we can write an elliptic curve E in Weierstrass Form,

$$y^2 = x^3 + ax + b, \text{ where } a, b \in \mathbb{F}_{p^2},$$

and define its j-invariant $j(E)$ as

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2}.$$

Then, over $\mathbb{F}_{p^2}$, two elliptic curves are identified (i.e., isomorphic) if and only if they have the same j-invariant. Isogenies define graph structures on the set of j-invariants, so-called *isogeny graphs* which nodes are the j-invariants of isogenous curves and which edges are isogenies connecting curves from each of the nodes. Again, it is an interesting challenge to describe the structure of isogeny graphs without revealing enough information to determine concrete paths (i.e., isogeny chains) linking two nodes.

In this paper we develop some new results to help us better understand isogeny graphs, linking them to nonlinear recurrences over finite fields.

1.2. **Related Work.** We establish several conjectures that link isogeny graphs and nonlinear recurrences over finite fields. These relationships provide deeper insights into the endomorphism ring of a curve, contributing towards the resolution of the so-called *Endomorphism Ring Problem* which seeks a computational description of the endomorphism ring of a supersingular elliptic curve.

Eisentraeger et al. [8] proved (unsing a heuristic introduced by Kohel et al. [13]) the equivalence of the isogeny path and endomorphism ring problems under polynomial time reductions. Later, B. Wesolowski provided an alternative proof that, instead of relying on heuristics, assumed the generalized Riemann hypothesis (see [21]). This result was subsequently refined by Mamah in [15], where the polynomial equivalence between the two problems was established without using heuristics or the generalized Riemann hypothesis.

2. 2-isogenies of elliptic curves

Let $p \geq 5$ be a prime such that $p \equiv 3 \pmod 4$ and $p \equiv 1 \pmod 3$, or equivalently, $p \equiv 7 \pmod{12}$. These conditions will be needed later. We denote the ground field $\mathbb{F}_p$

and its quadratic extension $\mathbb{F}_{p^2}$. We represent the elements of $\mathbb{F}_{p^2}$ by adjoining $\mathbf{i} = \sqrt{-1}$ to the base field $\mathbb{F}_p$, as the fact that $p \equiv 3 \pmod 4$ guarantees that -1 is not a square in $\mathbb{F}_p$. Hence $\mathbb{F}_{p^2} = \mathbb{F}_p[\mathbf{i}]$. Note that all elements of $\mathbb{F}_p$ have square roots in $\mathbb{F}_{p^2}$, but not all elements of $\mathbb{F}_{p^2}$ have square roots in $\mathbb{F}_{p^2}$. Finally let $K = \overline{\mathbb{F}_p}$ be the algebraic closure of $\mathbb{F}_p$, which is a separable extension of $\mathbb{F}_p$.

An elliptic curve E over K is expressed in short Weierstrass form as

$$E : y^2 = x^3 + ax + b,$$

where $a, b \in K$ satisfy that the discriminant $\Delta = 4a^3 + 27b^2 \neq 0$. The j-invariant is defined by

$$j = j(E) = 1728 \, \frac{4a^3}{4a^3 + 27b^2} \, .$$

We say that E lives over $\mathbb{F}_{p^m} \subset K$ if it can be written in short Weierstrass form with $a, b \in \mathbb{F}_{p^m}$. In this case, $j \in \mathbb{F}_{p^m}$. The converse follows from the explicit expressions given in section 3.

There is an hyperelliptic quotient

$$\pi : E \to \mathbb{P}^1, \qquad \pi(x, y) = x$$

which is a degree-2 map. We note that the x-coordinate x_P of a point P determines the y-coordinate up to sign.

We are interested in 2-isogenies between such elliptic curves. A 2-isogeny is a degree-2 separable isogeny $\psi : E \to E'$ with kernel of order 2, that is $\ker(\psi) = \{O, P\}$, where P is a point of order 2. Here O is the origin of E, which is the point at infinity, and it has coordinate $x_O = \infty$. The degree of an isogeny is actually its degree as a morphism of algebraic curves, and, moreover, for a separable isogeny this is equal to the cardinality of the kernel (see [18]). Note that even if E lives over $\mathbb{F}_{p^m}$, the point P can live over a field extension. And the elliptic curves E and E' can live over different subfields of K.

The elliptic curve E has always three points of order 2 over K, each point having (affine) x-coordinate one of the three distinct roots of $x^3 + ax + b = 0$. Let P be any such point of order 2 and let x_P be the x-coordinate of P. We consider the 2-isogeny $\psi : E \to E'$ with kernel $\ker(\psi) = \{O, P\}$, which determines E' univocally. Write $E' : y'^2 = x'^3 + a'x + b'$ in Weierstrass form.

Let $\pi' : E' \to \mathbb{P}^1$ be the hyperelliptic quotient associated to E'. Then ψ determines a map $\bar{\psi} : \mathbb{P}^1 \to \mathbb{P}^1$ on the x-coordinates, so that

$$\pi' \circ \psi = \bar{\psi} \circ \pi \, ,$$

that is, $(x', y') = \psi(x, y)$ and $x' = \bar{\psi}(x)$. This is easy to see: the hyperelliptic quotient is determined by the linear system $|2O| = |2P|$, hence the map $\pi' \circ \psi$ is determined by $|2O + 2P| = |2(O + P)|$. Hence the map $\bar{\psi} : \mathbb{P}^1 \to \mathbb{P}^1$ of degree 2 that sends x_P and $x_0 = \infty$ to ∞, does the job.

Moreover, the map $\bar{\psi}$ clearly determines the map ψ up to sign, since y' is determined by $y' = \sqrt{x'^3 + a'x + b'}$, up to sign.

Proposition 2.1. *There is some $\alpha \in K$, $\alpha \neq 0$, such that*

$$\bar{\psi}(x) = \alpha x + \frac{\alpha(3x_P^2 + a)}{x - x_P}. \tag{1}$$

The curve E' has Weierstrass equation

$$E' : y^2 = x^3 + \alpha^2(-4a - 15x_P^2)x + \alpha^3(-8ax_P - 22x_P^3). \tag{2}$$

Proof. The map $\bar{\psi}$ sends ∞, x_P to ∞, so it is clearly of the form $\bar{\psi} = \alpha x + \dfrac{\beta}{x - x_P}$. The expression (1) can be derived from Vélu's formulas [19] by direct substitution using the kernel point $(x_P, 0)$. The factor α is then added to consider composition of the Vélu isogeny with automorphisms. This determines the coefficient $\beta = \alpha(3x_P^2 + a)$ to arrange that the coefficient of x^2 for E' vanishes. The explicit expression of the codomain curve E' can be found in [17, Section 4]. □

For a 2-isogeny $\psi : E \to E'$, there is always another isogeny $\psi^* : E' \to E$ called the dual of ψ, The dual isogeny is defined by the property that $\psi^* \circ \psi = [2] : E \to E$ is the map defined by "multiplication by 2" on the elliptic curve. The map [2] has kernel $\{O, P_0, P_1, P_2\}$, where P_0, P_1, P_2 are the three points of order 2, hence if ψ is given by $P = P_0$, then ψ^* is determined by the order 2 point $P' = \psi(P_1) = \psi(P_2) \in E'$. The existence of the dual isogeny of a separable isogeny is guaranteed when working over a finite field.

Now let $\psi : E \to E'$ given by (1). Then ψ^* is defined by the map

$$\bar{\psi}^*(x) = \frac{1}{4}\,\frac{x}{\alpha} - \frac{\dfrac{3}{4}x_P^2 + a}{\dfrac{x}{\alpha} + 2x_P}\,. \tag{3}$$

The correctness of (3) for the dual isogeny can be easily checked by composing both isogenies and verifying that the result is the isogeny [2], whose expression appears in [17, eqn. (1)], since

$$\bar{\psi}^* \circ \bar{\psi}(x) = [\bar{2}](x) = \frac{1}{4}\,\frac{x^4 - 2ax^2 - 8bx + a^2}{x^3 + ax + b}\,.$$

From the expression (3) for the dual isogeny, it is immediate to see that its kernel is $\ker(\psi^*) = \{O, Q_0\}$, generated by a point $Q_0 \in E'$ of order 2 with x-coordinate

$$x_{Q_0} = -2\alpha x_P \,. \tag{4}$$

In this paper, we will focus on *supersingular* elliptic curves. There are many definitions of supersingular elliptic curves, for instance that the kernel of the map $[p] : E \to E$ is trivial. The key fact that we will use is that if $\psi : E \to E'$ is a 2-isogeny and E is supersingular, then E' is also supersingular. Moreover, if E is supersingular then $j(E) \in \mathbb{F}_{p^2}$ (see [18, Theorem V.3.1]), therefore supersingular curves are defined over $\mathbb{F}_{p^2}$.

3. The root form of an elliptic curve

The j-invariant classifies elliptic curves defined over K up to isomorphism. As it may be convenient to work with a fixed representative of each class, some authors have proposed definitions of "generic" formulas for a curve expressed in short Weierstrass form based on its j-invariant. For instance Connell [5] writes

$$y^2 + xy = x^3 - \frac{36}{j - 1728}x - \frac{1}{j - 1728}\,.$$

Another formula, proposed by Hasegawa [11], is

$$y^2 = x^3 - \frac{27j}{j - 1728}x + \frac{54j}{j - 1728}\,,$$

or Washington [20] proposes

$$y^2 = x^3 + \frac{3j}{1728 - j}x + \frac{2j}{1728 - j}\,.$$

An inconvenient of these proposals is that they do not contemplate the case $j = 1728$. We would like to work with a formula that includes this case as $p \equiv 3 \pmod 4$ guarantees that $j = 1728$ corresponds to a supersingular curve. For this reason, we consider working with a new expression for a curve with j-invariant j as follows:

$$E(j) : y^2 = x^3 + jk^2x \pm \frac{2}{3\sqrt{-3}}jk^3\sqrt{j - 1728}\,.$$

It is immediate to check that such curve has j-invaritant j for any value of k and any chosen sign for the square roots (note that this expression does not define the sign of either square root, therefore this definition actually corresponds to two isomorphic curves). Clearly this form is not valid for $j = 0$ since the formula would yield the

equation $y^2 = x^3$ which is singular and thus does not represent an elliptic curve. However the selection $p \equiv 1 \pmod 3$ guarantees that the value $j = 0$ does not correspond to a supersingular curve.

The parameter k may be chosen constant or it may depend on j. As the latter complicates the analysis considerably, we will choose it constant and for convenience we select $k = \frac{\sqrt{-1}}{24}$ which makes

$$E(1728) : y^2 = x^3 - 3x\,. \tag{5}$$

We name the resulting equation as follows.

Definition 3.1. We say that the elliptic curve $E = E(j)$ with j-invariant j is written in *root form* if we write the equation

$$E(j) : y^2 = x^3 - \frac{j}{576}x - \frac{j\sqrt{j-1728}}{20736\sqrt{3}}\,. \tag{6}$$

The name "root form" comes from the fact that it involves the root $\sqrt{j-1728}$. Note that if $j \in \mathbb{F}_{q^m}$, then the root form is an equation over $\mathbb{F}_{q^{2m}}$. However, the curve $E(j)$ is defined over $\mathbb{F}_{q^m}$.

The discriminant of a curve in root form is:

$$\Delta = 4\left(-\frac{j}{576}\right)^3 + 27\left(-\frac{j\sqrt{j-1728}}{20736\sqrt{3}}\right)^2 = -\frac{j^2}{27648}\,. \tag{7}$$

4. 2-isogenies between curves in root form

In expression (1), different values of α result in different codomain curves which are isomorphic to one another. We now find the value of α that defines a 2-isogeny from E to E' when both are expressed in root form. We begin by analyzing the case $x_P = 0$. The fact that $(0, 0)$ is a point of order two implies that the equation of the curve must be of the form $E : y^2 = x^3 + ax$, i.e., $b = 0$. According to (5) for E to be in root form we must have $a = -3$. The codomain E' is obtained from (2), say

$$E' : y^2 = x^3 + 12\alpha^2 x\,.$$

Since the j-invariant of the codomain is $j' = 1728$, we have that ψ is a morphism between curves with j-invariant 1728. To make this an endomorphism in $E(1728)$, we must have E' also expressed as (5) which yields $\alpha = \pm\mathbf{i}/2$.

The general case when $x_P \neq 0$ is contained in the following result.

Proposition 4.1. *Let x_P be the x-coordinate of a point of order two in a curve $E(j)$ in root form. Assume that $x_P \neq 0$. Let $\epsilon = \dfrac{j}{x_P^2}$ and let*

$$\alpha = \frac{12\sqrt{3}\,(2160-\epsilon)}{x_P\,(432-\epsilon)\sqrt{1728-\epsilon}} = \frac{12\sqrt{3}\,(2160\,x_P^2-j)}{(432\,x_P^2-j)\sqrt{1728\,x_P^2-j}}\,. \tag{8}$$

Then the isogeny $\psi : E \to E'$ has codomain curve E' with j-invariant j' which satisfies:

$$\sqrt{j'-1728} = \frac{2592\,(1584-\epsilon)}{(432-\epsilon)\sqrt{1728-\epsilon}}\,. \tag{9}$$

Proof. Substituting the expression (8) for α and the value $a = -\dfrac{j}{576}$ in (2) we get the curve

$$E' : y^2 = x^3 - 3\frac{(2160-\epsilon)^3}{(432-\epsilon)^2(1728-\epsilon)}x + \frac{216}{\sqrt{3}}\frac{(2160-\epsilon)^3(\epsilon-1584)}{(432-\epsilon)^3(1728-\epsilon)^{3/2}}\,. \tag{10}$$

The j-invariant is

$$j' = 1728\frac{(2160-\epsilon)^3}{(432-\epsilon)^2(1728-\epsilon)}\,, \tag{11}$$

from where (9) follows directly. The root form (6) of a curve with j-invariant j' is

$$y^2 = x^3 - \frac{j'}{576}x - \frac{j'\sqrt{j'-1728}}{20736\sqrt{3}}\,, \tag{12}$$

which is the same expression as (10). This concludes the proof. □

Remark 4.2. Formally, the result in Proposition 4.1 covers the case $x_P = 0$, where $j = 1728$, $\epsilon = \infty$, $\alpha = \dfrac{12\sqrt{3}}{\sqrt{-1728}} = \pm\mathbf{i}/2$ and $j' = 1728$.

There are two values of α in (8) as the square root is defined up to sign.

We call the 2-isogeny $\psi : E(j) \to E(j')$ between two curves in root form a "root isogeny". From (1), using the value (8) and $a = -\dfrac{j}{576}$, we have

$$\bar{\psi}(x) = \frac{16\,(2160\,x_P^2-j)}{\sqrt{3}\,(432\,x_P^2-j)\sqrt{1728\,x_P^2-j}}\left(x + \frac{1728x_P^2-j}{x-x_P}\right).$$

Regarding expressions (8), (9) and (11), we point out that, although the definition of α and the result for j' are undefined for $\epsilon = 432$ or $\epsilon = 1728$, it is easy to check that these values of j correspond to null discriminant for the codomain curve.

5. Chains of 2-isogenies

We now turn our interest to the composition of 2-isogenies using root isogenies, and in particular to the construction of a "chain" of 2-isogenies by repeated composition of root isogenies to obtain an isogeny of degree 2^ℓ. Formally, we may define a chain as a 2-regular graph where the nodes are associated with j-invariants and the edges are associated with root isogenies.

We start by characterizing the points of order two in the codomain curve in root form according to the following.

Proposition 5.1. *Let $E(j)$, x_P and ϵ be as defined in Proposition 4.1. Let $\psi : E \to E'$ be the root isogeny defined by x_P with codomain E'. Then the three values of the x-coordinates x_{Q_0}, x_{Q_1} and x_{Q_2} that correspond to the three points of order two in E' are:*

$$\{-2\alpha x_P, \alpha x_P(1+\eta), \alpha x_P(1-\eta)\}\,, \tag{13}$$

where $\eta = \dfrac{1}{12}\sqrt{1728-\epsilon}$.

Proof. We evaluate the expression $(x - x_{Q_0})(x - x_{Q_1})(x - x_{Q_2})$ and obtain:

$$x^3 - \alpha^2 x_P^2(3+\eta^2)x + 2\alpha^3 x_P^3(1-\eta^2)\,.$$

Substituting (8) and $\eta^2 = \dfrac{1}{144}(1728-\epsilon)$, we get (10). □

According to (4), the value $x_{Q0} = -2\alpha x_P$ corresponds to the dual isogeny which maps E' back to E. the other two values

$$x_{Q_1} = \alpha x_P(1+\eta), \qquad x_{Q_2} = \alpha x_P(1-\eta)$$

may be used to define two new isogenies from E' to some other curves E_1'' and E_2''. The values $\alpha x_P(1 \pm \eta)$ may be rewritten using (8) as:

$$\alpha x_P \pm \frac{12\sqrt{3}\,(2160-\epsilon)}{(432-\epsilon)\sqrt{1728-\epsilon}}\,\frac{\sqrt{1728-\epsilon}}{12} = -\frac{1}{2}x_{Q_0} \pm \sqrt{3}\,\frac{2160-\epsilon}{432-\epsilon}\,. \tag{14}$$

We point out that in our construction x_{Q_1} and x_{Q_2} are always different, since by our definition in Proposition 2.1 $\alpha \neq 0$ which implies $\epsilon \neq 2160$.

A chain of 2-isogenies may thus be built using root isogenies by selecting either x_{Q_1} or x_{Q_2} at every step. The process is defined recurrently as follows:

(1) Assume that we have arrived at a curve $E_n = E(j_n)$ from a previous curve $E_{n-1} = E(j_{n-1})$ via the root isogeny $\psi : E_{n-1} \to E_n$, using the order 2 point P_{n-1}. Then j_n is given by (11) with $\epsilon_{n-1} = \dfrac{j_{n-1}}{x^2_{P_{n-1}}}$.

(2) The curve $E_n = E(j_n)$ has three points of order two whose x-coordinates are $x_{Q_{n,i}}$, $i = 0, 1, 2$. One of the points $x_{Q_{n,0}}$ brings us back to E_{n-1} via the dual isogeny ψ^*. We focus on the other two points $x_{Q_{n,1}}$ and $x_{Q_{n,2}}$, and select one of them as x_{P_n}.

(3) The choice of x_{P_n} defines the value $\epsilon_n = \dfrac{j_n}{x^2_{P_n}}$, and the root isogeny $\psi : E_n \to E_{n+1}$, thus determining the next value j_{n+1} and the next curve in the chain $E_{n+1} = E(j_{n+1})$.

6. Chain of supersingular curves

We are interested in the case of a chain of 2-isogenies consisting of *supersingular* elliptic curves. If E_1 is supersingular, then all curves E_n in the chain will be supersingular. In particular all $j_n \in \mathbb{F}_{p^2}$ and all the curves are defined over $\mathbb{F}_{p^2}$.

We will start a chain with the curve

$$E_1 = E(1728) : y^2 = x^3 - 3x.$$

From this curve and using either value of $x_P = \pm\sqrt{3}$, we obtain using (8) for the root isogeny with $\epsilon_1 = \dfrac{j_1}{x_P^2} = 576$,

$$\alpha_1 = \frac{12\sqrt{3}}{x_P} \frac{2160 - \epsilon_1}{(432 - \epsilon_1)\sqrt{1728 - \epsilon_1}} = \mp\frac{11}{2\sqrt{2}},$$

which maps to the codomain curve E_2 with j-invariant given by (11)

$$j_2 = 1728\frac{(2160 - \epsilon_1)^3}{(432 - \epsilon_1)^2(1728 - \epsilon_1)} = 66^3.$$

The curve equation is given by (6)

$$E_2 : y^2 = x^3 - \frac{j_2}{576}x - \frac{j_2\sqrt{j_2 - 1728}}{20736\sqrt{3}} = x^3 - \frac{3}{8}11^3\, x \pm \frac{21\sqrt{3}}{8\sqrt{2}}11^3.$$

Thus from $E_1 = E(1728)$ both points $x_P = \pm\sqrt{3}$ define the same root isogeny that maps to $E_2 = E(66^3)$. We note that this is consistent with the fact that we have a 3-regular graph, as the node $j_1 = 1728$ also has an edge to itself corresponding to $x_P = 0$. See Figure 3 below for the graph of isogenies at this node.

Then from E_2 we define the chain by selecting at each step one of the two possibilities in (14). According to (13), and using $x_P = \pm\sqrt{3}$, $\epsilon_1 = 576$, $\eta = \dfrac{\sqrt{1728-\epsilon_1}}{12} = 2\sqrt{2}$, $\alpha_1 = \dfrac{11}{2\sqrt{2}}$, we have that the three x-coordinates of points of order two in E_2 are

$$\left\{-11\sqrt{\frac{3}{2}}, \frac{11}{4}\sqrt{3}(\sqrt{2}+2), \frac{11}{4}\sqrt{3}(\sqrt{2}-2)\right\}.$$

The first point corresponds to the dual isogeny that brings us back to E_1, and the last two points may be used to map to a new curve E_3.

Theorem 6.1. *Let x_{P_n} be the x-coordinate of a point of order two in a curve $E_n = E(j_n)$ in root form. Let $\psi : E_n \to E_{n+1}$ be the root isogeny defined by x_{P_n}, where $E_{n+1} = E(j_{n+1})$ is the codomain of the root isogeny, and let $x_{Q_{n,i}}$, $i = 1, 2$, be the x-coordinates of the points of order two in E_{n+1}.*

Assume that $j_n \neq 1728$, $\sqrt{j_n - 1728} \in \mathbb{F}_{p^2}$, and $x_{P_n} \in \mathbb{F}_{p^2}$ with $x_{P_n} \neq 0$. Then the following are true:

(1) $\sqrt{j_{n+1} - 1728} \in \mathbb{F}_{p^2}$,
(2) $x_{Q_n,i} \in \mathbb{F}_{p^2}$, *for* $i = 0, 1, 2$,

Proof. We begin by proving (a). Recall that by definition x_{P_n} is any one of the three solutions of the cubic

$$x^3 - \frac{j_n}{576}x - \frac{j_n\sqrt{j_n - 1728}}{20736\sqrt{3}} = 0\,. \tag{15}$$

Let us call the roots of this cubic x_1, x_2, x_3 and, without loss of generality, assume $x_1 = x_{P_n}$.

Since, by hypothesis, $\sqrt{j_n - 1728} \in \mathbb{F}_{p^2}$, the cubic has all its coefficients in $\mathbb{F}_{p^2}$. The discriminant of this cubic was given in (7) as $\Delta = -\dfrac{j_n^2}{27648}$, which is a square in $\mathbb{F}_{p^2}$. By [7, Lemma 2], the discriminant of a cubic is not a square in $\mathbb{F}_{p^2}$ if and only if it has exactly one root in $\mathbb{F}_{p^2}$. Applied to this case, we get that (15) does not have exactly one root. Since it has already one solution in $\mathbb{F}_{p^2}$, namely $x_1 = x_{P_n} \in \mathbb{F}_{p^2}$, then at least one of x_2, x_3 must also be in $\mathbb{F}_{p^2}$. As $x_1 + x_2 + x_3 = 0$, this implies that also $x_3 \in \mathbb{F}_{p^2}$.

Call $\epsilon_i = \dfrac{j_n}{x_i^2}$, $i = 1, 2, 3$. Using equation (11), we get

$$j_{n+1} = 1728\frac{(2160-\epsilon_i)^3}{(432-\epsilon_i)^2(1728-\epsilon_i)} \in \mathbb{F}_{p^2}\,.$$

Moreover, operating the above expression, we get that ϵ_i are the three roots of the cubic equation

$$(1728 - j_{n+1})\epsilon^3 + 2592\,(j_{n+1} - 4320)\epsilon^2 + \\ + 1679616\,(14400 - j_{n+1}) + 322486272\,(j_{n-1} - 54000) = 0\,. \qquad (16)$$

We recall that for a cubic in general form $a\,\epsilon^3 + b\,\epsilon^2 + c\,\epsilon + d$, the discriminant is calculated as

$$\Delta = b^2c^2 - 4\,ac^3 - 4\,b^3d - 27\,a^2d^2 + 18\,abcd\,.$$

Applying this formula to (16) we get the discriminant

$$\Delta_\epsilon = 2^{38}3^{24}j_{n+1}^2(j_{n+1} - 1728)\,.$$

The cubic (16) has three roots $\epsilon_1, \epsilon_2, \epsilon_3$ and they lie in $\mathbb{F}_{p^2}$. Therefore, using the result in [7, Lemma 2] again, we have that Δ_ϵ is a square in $\mathbb{F}_{p^2}$. This implies that $\sqrt{j_{n+1} - 1728} \in \mathbb{F}_{p^2}$.

Now we prove (b). Since $x_{P_n} \in \mathbb{F}_{p^2}$ and $j_n \in \mathbb{F}_{p^2}$, we have $\epsilon_n = \dfrac{j_n}{x_{P_n}^2} \in \mathbb{F}_{p^2}$. Using (9) and $\sqrt{j_{n+1} - 1728} \in \mathbb{F}_{p^2}$, we have that $\sqrt{1728 - \epsilon_n} \in \mathbb{F}_{p^2}$. From (8), we have $\alpha_n \in \mathbb{F}_{p^2}$. According to (4), we have that $x_{Q_{n,0}} = -2\alpha_n x_{P_n} \in \mathbb{F}_{p^2}$. Now, according to (14)

$$x_{Q_{n,i}} = -\frac{1}{2}x_{Q_{n,0}} \pm \sqrt{3}\,\frac{2160 - \epsilon_n}{432 - \epsilon_n} \in \mathbb{F}_{p^2}\,,$$

for $i = 1, 2$. Therefore $x_{Q_{n,i}} \in \mathbb{F}_{p^2}$, for $i = 0, 1, 2$. □

Note that in Theorem 6.1, if $j_n = 1728$ then the discussion previous to the theorem assures that the result also holds. In the case $x_{P_n} = 0$ then $j_n = 1728$ and the 2-isogeny is from $E(1728)$ to itself. In both cases, the conclusion also holds.

Corollary 6.2. *For all curves E_n in a chain we have $\sqrt{j_n - 1728} \in \mathbb{F}_{p^2}$ and $x_{P_n} \in \mathbb{F}_{p^2}$.*

Proof. We proceed by induction starting with the curve E_2. For E_2 we have that $j_2 = 66^3 \neq 1728$ and $\sqrt{j_2 - 1728} = 378\sqrt{2} \in \mathbb{F}_{p^2}$ and $x_{P_2} = \dfrac{11}{4}\sqrt{3}(\sqrt{2} + 2) \in \mathbb{F}_{p^2}$. As $x_{P_2} \neq 0$, we have by Theorem 6.1 that $\sqrt{j_3 - 1728} \in \mathbb{F}_{p^2}$ and $x_{Q_{2,i}} \in \mathbb{F}_{p^2}$ for the three points of order 2. Note that we choose P_3 as either $Q_{2,1}$ or $Q_{2,2}$, so $x_{P_3} \in \mathbb{F}_{p^2}$.

We continue the process recursively. If we have $j_n \neq 1728$, then we apply Theorem 6.1. If at some stage, $j_n = 1728$ then the result also holds by the discussion above. □

Remark 6.3. As $\sqrt{j_n - 1728} \in \mathbb{F}_{p^2}$, we have that (12) is an equation for $E(j_n)$ defined over $\mathbb{F}_{p^2}$.

7. A recurrence associated with a chain of 2-isogenies

In Proposition 5.1 we defined $\eta = \frac{1}{12}\sqrt{1728-\epsilon}$. The interest of this value is highlighted in the following

Proposition 7.1. *For each $n \geq 1$, let x_{P_n} be the x-coordinate of a point of order two in the curve $E_n = E(j_n)$ expressed in root form. Let $\epsilon_n = \frac{j_n}{x_{P_n}^2}$, $\eta_n = \frac{1}{12}\sqrt{1728-\epsilon_n}$, and let $\psi : E_n \to E_{n+1}$ be the root isogeny defined by x_{P_n}, whose codomain curve is $E_{n+1} = E(j_{n+1})$. Then, with a suitable choice of sign for each η_n, we have the recurrence*

$$\eta_{n+1}^2 = 8\eta_n \frac{\eta_n + 3}{(\eta_n+1)^2}\,, \tag{17}$$

and all $\eta_n \in \mathbb{F}_{p^2}$.

Proof. From (8), we have

$$\alpha_n^2 x_{P_n}^2 = 432\frac{(2160-\epsilon_n)^2}{(432-\epsilon_n)^2(1728-\epsilon_n)}\,,$$

whence, using (11), we get

$$j_{n+1} = 4\alpha_n^2 x_{P_n}^2 (2160-\epsilon_n)\,.$$

From Proposition 5.1,

$$x_{P_{n+1}}^2 = \alpha_n^2 x_{P_n}^2 (1 \pm \eta_n)^2\,,$$

where the choice of sign indicates the two possible choices for the point $x_{P_{n+1}}$ in the curve E_{n+1}. Therefore

$$x_{P_{n+1}}^2 = \frac{j_{n+1}}{4(2160-\epsilon_n)}\,(1\pm\eta_n)^2\,.$$

This provides the following expression for ϵ_{n+1},

$$\epsilon_{n+1} = \frac{j_{n+1}}{x_{P_{n+1}}^2} = \frac{4(2160-\epsilon_n)}{(1\pm\eta_n)^2}\,.$$

Using the definition of η_n, we have $\epsilon_n = 1728 - 144\,\eta_n^2$. Substituting

$$\epsilon_{n+1} = 1728 - 144\eta_{n+1}^2 = \frac{4(2160-1728+144\eta_n^2)}{(1\pm\eta_n)^2} = \frac{576(\eta_n^2+3)}{(1\pm\eta_n)^2}\,,$$

and

$$\eta_{n+1}^2 = 12 - \frac{4(\eta_n^2+3)}{(1\pm\eta_n)^2} = 8\eta_n\frac{\eta_n \pm 3}{(\eta_n\pm 1)^2}\,.$$

If the choice of sign is $+$, then we alredady have the recurrence

$$\eta_{n+1}^2 = 8\eta_n \frac{\eta_n + 3}{(\eta_n + 1)^2}\,.$$

if the choice of sign is $-$, then we change η_n by $\eta'_n = -\eta_n$ (that is, we interchange the role of the two points $Q_{n,i}$, $i = 1, 2$), and we have

$$\eta_{n+1}^2 = 8\eta_n \frac{\eta_n - 3}{(\eta_n - 1)^2} = -8\eta_n \frac{-\eta_n + 3}{(-\eta_n + 1)^2} = 8\eta'_n \frac{\eta'_n + 3}{(\eta'_n + 1)^2}\,.$$

The new value of η_n is an allowed choice for the previous step in the recurrence.

Finally, note that all $\eta_n \in \mathbb{F}_{p^2}$ since according to (9),

$$\eta_n = \frac{\sqrt{1728 - \epsilon_n}}{12} = \frac{216(1584 - \epsilon_n)}{(432 - \epsilon_n)\sqrt{j_{n+1} - 1728}}\,,$$

and according to Theorem 6.1, we have $\sqrt{j_{n+1} - 1728} \in \mathbb{F}_{p^2}$. □

Proposition 7.1 shows that a recurrence in the value η may be used to generate all the j-invariants in a 2-isogeny chain. Indeed, since at each step η^2 provides $\epsilon = 1728 - 144\,\eta^2$, we may substitute in (11) and obtain the following expression for the j-invariant:

$$j_{n+1} = 1728 \frac{(\eta_n^2 + 3)^3}{\eta_n^2(\eta_n^2 - 9)^2}\,. \tag{18}$$

The recurrence (17) can be simplified considerably using the change of variable

$$\mu_n = \frac{\eta_n + 3}{2\eta_n}\,, \qquad \eta_n = \frac{3}{2\mu_n - 1}\,. \tag{19}$$

This change of variable in (18) yields

$$j_{n+1} = 256 \frac{(\mu_n^2 - \mu_n + 1)^3}{(\mu_n^2 - \mu_n)^2}\,. \tag{20}$$

In particular, (19) transforms the recurrence in η_n into this equivalent recurrence in μ_n,

$$\mu_{n+1} = \frac{1}{2} + \frac{3}{2\eta_{n+1}} = \frac{1}{2} + \frac{3}{2\sqrt{\dfrac{8\eta_n(\eta_n + 3)}{(\eta_n + 1)^2}}} = \frac{1}{2} + \frac{3\dfrac{\eta_n + 1}{\eta_n}}{2\sqrt{\dfrac{8(\eta_n + 3)}{\eta_n}}} = \frac{1}{2} + \frac{3\left(1 + \dfrac{2\mu_n - 1}{3}\right)}{8\sqrt{\mu_n}}\,,$$

and finally

$$\mu_{n+1} = \frac{1}{2} + \frac{\mu_n + 1}{4\sqrt{\mu_n}}\,. \tag{21}$$

This recurrence provides two possible values of μ_{n+1} for each μ_n depending of the square root $\sqrt{\mu_n}$ that we select.

Note that the fact that all $\eta_n \in \mathbb{F}_{p^2}$ implies that all $\mu_n \in \mathbb{F}_{p^2}$ because of (19). On the other hand, (21) implies

$$\sqrt{\mu_n} = \frac{\mu_n + 1}{4\mu_{n+1} - 2}\,,$$

which shows that $\sqrt{\mu_n} \in \mathbb{F}_{p^2}$, or in other words, all μ_n are squares in $\mathbb{F}_{p^2}$. Let $\mu_n = u_n^2$, with $u_n \in \mathbb{F}_{p^2}$. Then (21) may be written as

$$u_{n+1}^2 = \frac{1}{2} + \frac{u_n^2 + 1}{4u_n} = \frac{(u_n + 1)^2}{4u_n}\,.$$

And we have the following recurrence for u_n,

$$u_{n+1} = \frac{u_n + 1}{2\sqrt{u_n}}\,. \tag{22}$$

Again, we may reason as before: since according to (22), we have $\sqrt{u_n} = \dfrac{u_n + 1}{2u_{n+1}}$, the fact that $u_n \in \mathbb{F}_{p^2}$ for all n, implies that u_n is a square in $\mathbb{F}_{p^2}$. Thus we may define $u_n = v_n^2$ with $v_n \in \mathbb{F}_{p^2}$, and write (22) in terms of v_n as

$$v_{n+1}^2 = \frac{1}{2}\left(v_n + \frac{1}{v_n}\right), \tag{23}$$

which is a suprisingly simple recurrence.

Theorem 7.2. *The chain of 2-isogenies E_n defines a recurrence given by $v_0 = \sqrt{\sqrt{2}}$ and*

$$v_{n+1}^2 = \frac{1}{2}\left(v_n + \frac{1}{v_n}\right).$$

The j-invariants are related to this recurrence by

$$j_{n+1} = 256\frac{(v_n^8 - v_n^4 + 1)^3}{(v_n^8 - v_n^4)^2}\,. \tag{24}$$

The two choices of sign of v_n corresponds to the two choices of 2-isogenies in the isogeny graph.

Proof. The change of variable $\mu_n = u_n^2$ and $u_n = v_n^2$ gives $\mu_n = v_n^4$, which we plug into (20) to get (24).

The chain of 2-isogenies start with $E_1 = E(1728)$, $E_2 = E(66^3)$. The value $j_1 = 1728$ with $x_{P_1} = \pm\sqrt{3}$ provides $\epsilon_1 = \dfrac{j_1}{x_{P_1}^3} = 576$. By the definition of η, we have $\eta_1 = 2\sqrt{2}$. At

this point, we may note that the recurrence (17) provides $\eta_1 = 2\sqrt{2}$ if we set $\eta_0 = 1$. For this reason we start the recurrence at index 0 instead of 1. By (19) and $\eta_0 = 1$, we get $\mu_0 = 2$. Therefore $v_0 = \sqrt[4]{2}$. Note that we can have obtained this value from $j_1 = 1728$ and (24).

The change of sign for v_n corresponds to the choice of square root for u_n, and by (22) this means a change of sign for u_{n+1}. This in turn is a choice of square root for μ_{n+1}, and produces a change of sign for $2\mu_{n+2} - 1$ by (21). By (19) this corresponds to changing the sign of η_{n+2}, that is interchanging the points $x_{Q_{n,i}}$, $i = 1, 2$. □

To the authors, it was remarkable that a recurrence as (23), which requires to extract square roots successively, it is defined for all n, always obtaining square roots in $\mathbb{F}_{p^2}$. This happens with the starting seed $v_0 = \sqrt[4]{2}$. A computational check shows that starting at other values, the recurrence typically stops (that is a square root lies in a higher extension field $\mathbb{F}_{p^{2n}}$, $n \geq 2$. We raise the following conjecture.

Conjecture 7.3. *Let $v_0 \in \mathbb{F}_{p^2}$ corresponding to the j-invariant $j_1 = 256\dfrac{(v_0^8 - v_0^4 + 1)^3}{(v_0^8 - v_0^4)^2}$. Then the curve $E(j_1)$ is supersingular if and only if for any recurrence (v_n) defined by (23), all $v_n \in \mathbb{F}_{p^2}$.*

Note that we have proved the "only if" direction. If Conjecture 7.3 is true, then this would produce a good heuristic test for a j-invariant to correspond to a supersingular curve.

8. A relation with the Arithmetic Geometric Mean

The recurrence (23) has not been found by the authors explicitly in the literature, but there is a relationship of this recurrence with the so called Arithmetic-Geometric Mean (AGM for short) which we now present.

The AGM recurrence (going back to Gauss [6]) is defined by some starting $a_0, b_0 \in \mathbb{K}$ and for $n \geq 1$, we take $a_n, b_n \in \mathbb{K}$ by

$$a_n = \frac{a_{n-1} + b_{n-1}}{2}, \tag{25}$$

$$b_n = \sqrt{a_{n-1} b_{n-1}}, \tag{26}$$

where $\mathbb{K}$ is a field. There is a choice of square root for b_n, giving rise to situations in which the AGM recurrence terminates (if there is no square root), or situations in which the AGM recurrence splits in a graph (taking either choice of sign for the square root).

The AGM recurrence has been studied in fields of characteristic zero, for instance in [12] for p-adic numbers. It is also mentioned in the literature [20, section 9.4.1], [18, exercise 6.14]. But the only result in finite fields known to the authors appears in [10] and is limited to the ground field $\mathbb{F}_p$. In this case, the fact that $p \equiv 3 \pmod 4$ guarantees that there is a unique choice of square root for b_n so that for the following step, b_{n+1} is defined in $\mathbb{F}_p$, that is $a_{n-1}b_{n-1}$ is a square in $\mathbb{F}_p$.

We note that [10] mentions the relation between the AGM and 2-isogenies of elliptic curves and their j-invariants, when curves are expressed in Montgomery form; however they limit their analysis to the base field $\mathbb{F}_p$. Here we tackle the AGM in the quadratic extension $\mathbb{F}_{p^2}$ and provide a condition for it to be well-defined in it.

Theorem 8.1. *Let v_n be the sequence defined by (23) starting at some $v_0 \in \mathbb{F}_{p^2}$. Let a_n, b_n, $n \geq 1$, defined by*

$$b_n = \prod_{i=0}^{n-1} v_i, \qquad a_n = v_n^2 b_n \,.$$

Then a_n, b_n are the sequences of the AGM recurrence (25), (26). Furthermore, a sufficient condition for the sequences a_n, b_n to be defined in $\mathbb{F}_{p^2}$ is that they are initiated using any v_0 (that is $b_1 = v_0$, $a_1 = v_1^2 v_0 = (v_0^2+1)/2$) that satisfies (see (24)) that

$$j = 256 \frac{(v_0^8 - v_0^4 + 1)^3}{(v_0^8 - v_0^4)^2}$$

is the j-invariant of a supersingular elliptic curve in $\mathbb{F}_{p^2}$.

Proof. The fact that $a_n, b_n \in \mathbb{F}_{p^2}$ is clear from their definition and the fact that $v_i \in \mathbb{F}_{p^2}$ for all $i \geq 0$, when we initiate correctly (that is, when the j-invariant of v_0 is associated to a supersingular elliptic curve, by Proposition 7.1).

It remains to prove that a_n, b_n satisfy (25) and (26). Clearly $b_n = b_{n-1}v_{n-1}$, hence

$$b_n^2 = b_{n-1}^2 v_{n-1}^2 = b_{n-1}^2 \frac{a_{n-1}}{b_{n-1}} = a_{n-1}b_{n-1} \,,$$

which is (25). Next, we use the defintion of a_n and the formula for the recurrence

$$v_n^2 = \frac{1}{2}\left(v_{n-1} + \frac{1}{v_{n-1}}\right) = \frac{a_n}{b_n} \,,$$

to get

$$b_n(v_{n-1}^2 + 1) = 2a_n v_{n-1} \,. \tag{27}$$

On the other hand, $a_{n-1} = v_{n-1}^2 b_{n-1} = v_{n-1}(v_{n-1}b_{n-1}) = v_{n-1}b_n$, that is $v_{n-1} = \dfrac{a_{n-1}}{b_n}$. Substituting in (27),

$$b_n \left(\frac{a_{n-1}^2}{b_n^2} + 1 \right) = 2a_n \frac{a_{n-1}}{b_n} \,,$$

which gives, using also (25),

$$a_n = \frac{a_{n-1}^2 + b_n^2}{2a_{n-1}} = \frac{a_{n-1}^2 + a_{n-1}b_{n-1}}{2a_{n-1}} = \frac{a_{n-1} + b_{n-1}}{2} \,,$$

proving (26). □

There is a converse construction. Let us consider a AGM sequence (a_n, b_n), that is a sequence satisfying (25) and (26). Let us define

$$v_n^2 = \frac{a_n}{b_n} \,.$$

This square root exists because $a_n b_n$ is a square, since b_{n+1} is defined. Then

$$v_n^2 = \frac{a_n}{b_n} = \frac{1}{2}\frac{a_{n-1} + b_{n-1}}{\sqrt{a_{n-1}b_{n-1}}} = \frac{1}{2}\left(\sqrt{\frac{a_{n-1}}{b_{n-1}}} + \sqrt{\frac{b_{n-1}}{a_{n-1}}} \right) = \frac{1}{2}\left(v_{n-1} + \frac{1}{v_{n-1}} \right) ,$$

for a suitable choice of square root (that is, sign of v_{n-1}). Note that the values of v_n can be expressed solely based on b_n, since

$$v_n = \sqrt{\frac{a_n}{b_n}} = \sqrt{\frac{a_n b_n}{b_n^2}} = \sqrt{\frac{b_{n+1}^2}{b_n^2}} = \frac{b_{n+1}}{b_n} \,.$$

Therefore, for $b_0 = 1$ we have $b_N = \prod_{i=0}^{N-1} v_i$.

Remark 8.2. Over the real numbers $\mathbb{R}$, the AGM sequence is used to define a function [6] M as

$$M(a_0, b_0) = \lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n \,,$$

for $a_0, b_0 > 0$. The AGM sequence is uniquely determined by selecting at each step the positive sign for b_n. It can be seen that (a_n), (b_n) both converge to the same number [6]. Therefore $v_n \in (0, 1)$ for $n > 0$, and it will converge to 1.

Note the fantastic coincidence with the famous sequence from Euler. This is the AGM sequence in $\mathbb{R}$ starting with $a_0 = \sqrt{2}$ and $b_0 = 1$ and leads to an explicit formula that computes π. This corresponds to $v_0 = \sqrt{\sqrt{2}}$, which is also our starting value in $\mathbb{F}_{p^2}$ for the sequence of 2-isogenies of supersingular elliptic curves.

9. The multigraph structure of the supersingular 2-isogeny graph

Chains of supersingular curves, as defined in previous sections, correspond to paths in supersingular 2-isogeny graphs. Supersingular isogeny graphs have been extensively discussed in the literature and we do not intend to discuss them here. However we wish to review some features regarding their multigraph nature which has been less thoroughly analyzed (see for instance [9, 2]).

We recall that a supersingular 2-isogeny graph is a graph whose vertices or nodes are the isomorphism classes of supersingular elliptic curves over a finite field and whose edges represent degree-2 isogenies between them [17, Section 4]. Thus, each node corresponds to a supersingular elliptic curve (up to isomorphism), and thus with a j-invariant, while an edge connects two nodes if there is a separable isogeny of degree 2 between the corresponding curves. If we identify each isogeny with its dual isogeny (in the sense that an edge represents both), we may treat the graph as undirected. Furthermore the graph is known to be connected and in fact an expander (a Ramanujan graph) in large characteristic.

Since every supersingular elliptic curve has exactly 3 subgroups of order 2, it follows that from each node emanate three degree-2 isogenies. Thus the graph is 3-regular in a multigraph sense. By multigraph we mean that some edges may become self-loops (edges from a node to itself arising from special self-isogenies) or multiple edges (arising when two distinct 2-isogenies connect the same pair of curves, therefore in this case double edges). Most nodes in the graph do not exhibit these anomalies, but a few special nodes do. We are interested in discussing both self-loops and double edges and derive some results that will be useful later when we discuss cycles in these graphs.

A powerful tool for this analysis is the classical modular equation. For a given integer N, the modular equation $\Phi_N(X, Y) = 0$ characterizes pairs of j-invariants corresponding to elliptic curves linked by a cyclic isogeny of degree N. For 2-isogenies, the equation $\Phi_2(X, Y)$ is given by [14, Chapter 3] as

$$\begin{aligned}\Phi_2(X,Y) = {} & (X+Y)^3 - X^2Y^2 + 1485\,XY(X+Y) - 162000\,(X+Y)^2 \\ & + 41097375\,XY + 8748000000\,(X+Y) - 157464000000000. \end{aligned} \tag{28}$$

This equation relates any two j-invariants which are connected by an edge in the supersingular 2-isogeny graph.

By simple substitution it may be checked that the following change of variable

$$\frac{36\,(X+Y)+4671675}{2205225} = t^2+2\,,$$
$$\frac{216XY-160380\,(X+Y)-4438516500}{3274759125} = t^3+3\,t\,,$$

always satisfies the equation. Thus t parameterizes the equation $\Phi_2\,(X,Y)=0$. For reasons we will later justify, we prefer to change the parameter t to a parameter g defined as

$$g = \frac{495}{2}(t+1)\,,$$

which yields

$$XY = g^3\,,$$
$$X+Y = g^2-495\,g+54000\,.$$

Equivalently, any two adjacent j-invariants in the supersingular 2-isogeny graph are the roots of the following quadratic equation:

$$j^2-\left(g^2-495g+54000\right)j+g^3=0\,. \tag{29}$$

The interpretation of this equation is as follows. The value g characterizes a particular edge in the graph. Hence, given a suitable value of g, the two j-invariants connected by that edge are obtained by finding the roots of the quadratic equation (29). Likewise, given a j-invariant we may find the three edges out of it, characterized by their value g, by solving the cubic

$$g^3-j\,g^2+495j\,g+(j^2-54000j)=0.$$

Now it is obvious why the parameter g has been selected. According to Vieta's formulas, the sum of the three values of g out of any node provide the node j-invariant j.

We are now in a position to analyze self loops and double edges.

9.1. **Self loops.** Self loops correspond to j-invariants j that satisfy $\Phi_2\,(X,Y)=0$ when $X=Y=j$. Substituting in equation (28) one obtains:

$$(j-8000)\,(j-1728)\,(j+3375)^2=0.$$

We start by analyzing the cases $j=1728$ and $j=-3375$. These have in common that both correspond to a double root in the cubic, which we know by checking that they make its discriminant null. The discriminant of the cubic is

$$18j^3\,(495)\,(54000-j)+4j^4\,(j-54000)+495^2j^4-4\left(495^3\right)j^3-27j^2\,(j-54000)^2=0,$$

which simplifies to

$$4j^2\,(j-1728)\,(j+3375)^2=0.$$

Because of our selection of the characteristic p, we know that the value $j=0$ does not correspond to a supersingular curve. The values $j=1728$ and $j=-3375$ constitute "pure" self loops (see Remark 9.1 for a comment on this) in the graph as shown in the figure below (numbers in nodes correspond to values of j and values in edges correspond to values of g).

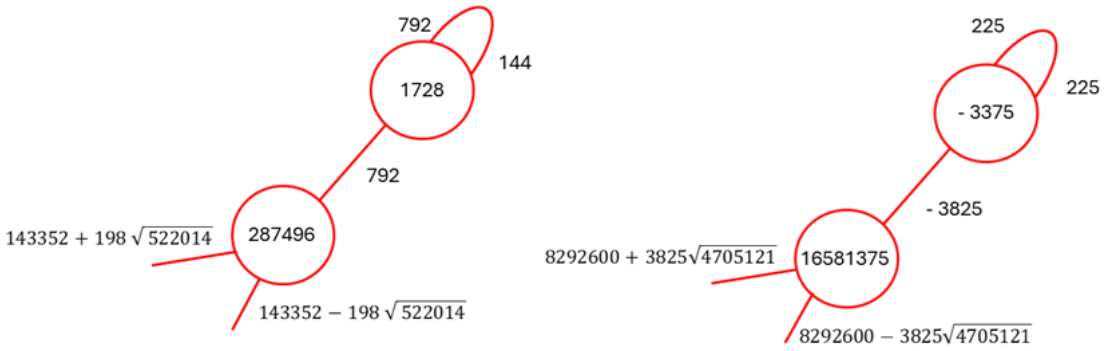

FIGURE 1. Self loops corresponding to $j=1728$ and $j=-3375$.

We now analyze the remaining case $j=8000$ which we shall see is a bit different. Substituting this value in the cubic we obtain

$$(g-400)\left(g^2-7600g+920000\right)=0.$$

The value $g=400$ constitutes the self-loop, since when substituted in (29), it yields

$$(j-8000)^2=0.$$

The value $j=8000$ is a special node in the graph as shown in the figure below.

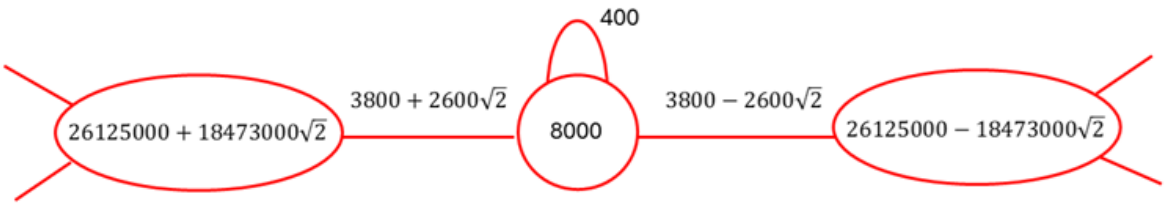

FIGURE 2. Self loop corresponding to $j=8000$.

Remark 9.1. Figure 2 may cause some confusion as node $j = 8000$ apparently has four edges instead of three. What is really happening is the following. In a "pure" self loop we find two values for g which represent two different self-isogenies, namely one and its dual. However the self-isogeny represented by $g = 400$ is its own dual, hence there are still only three 2-isogenies out of this node.

9.2. **Double edges.** In order to identify double edges we need to impose that there are two different solutions of g that satisfy the quadratic equation (29). For this purpose let us first see how we would go about obtaining the value g corresponding to two j-invariants (j_1, j_2). First we would add the j invariants and solve g for

$$g^2 - 495\, g + 54000 - j_1 - j_2 = 0.$$

This provides two values for g given by

$$g = \frac{1}{2}\left(495 \pm \sqrt{29025 + 4\,(j_1 + j_2)}\right). \tag{30}$$

And the correct value of g is the one that further satisfies the condition $g^3 = j_1 j_2$.

A double edge occurs when both values of g are different and both satisfy this condition, i.e.,

$$\left(\frac{1}{2}\left(495 + \sqrt{29025 + 4\,(j_1 + j_2)}\right)\right)^3 = \left(\frac{1}{2}\left(495 - \sqrt{29025 + 4\,(j_1 + j_2)}\right)\right)^3.$$

After simplification this becomes

$$(764100 + 4(j_1 + j_2))\,\sqrt{29025 + 4\,(j_1 + j_2)} = 0.$$

In the expression above a null radicand corresponds to the same value of $g = 495/2$. As we seek two different values for g (one for each edge) the condition becomes $j_1 + j_2 = -191025$. Substituting in the expression (30) we have the two solutions

$$g = 495\,\frac{1 \pm \sqrt{-3}}{2},$$

and both solutions provide the same value

$$g^3 = -495^3 = -121287375.$$

Since $j_1 + j_2 = -191025$ and $j_1 j_2 = -495^3$, we obtain that double edges correspond to the values of j given by the solutions of

$$j^2 + 191025j - 121287375 = 0\,.$$

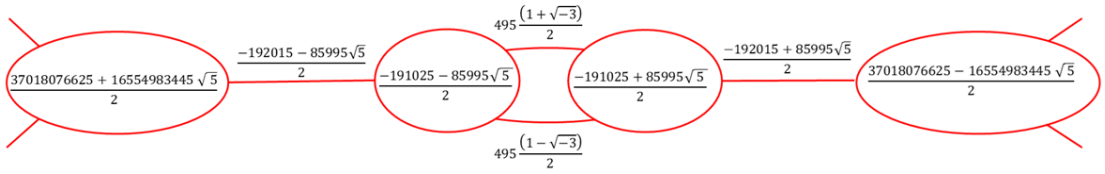

FIGURE 3. Double edge.

The special cases discussed above involve values of j which may or may not correspond to supersingular curves, depending on the field characteristic. The lowest value of the characteristic that we have found to involve all the cases corresponds to $p = 103$ (see Figure 4).

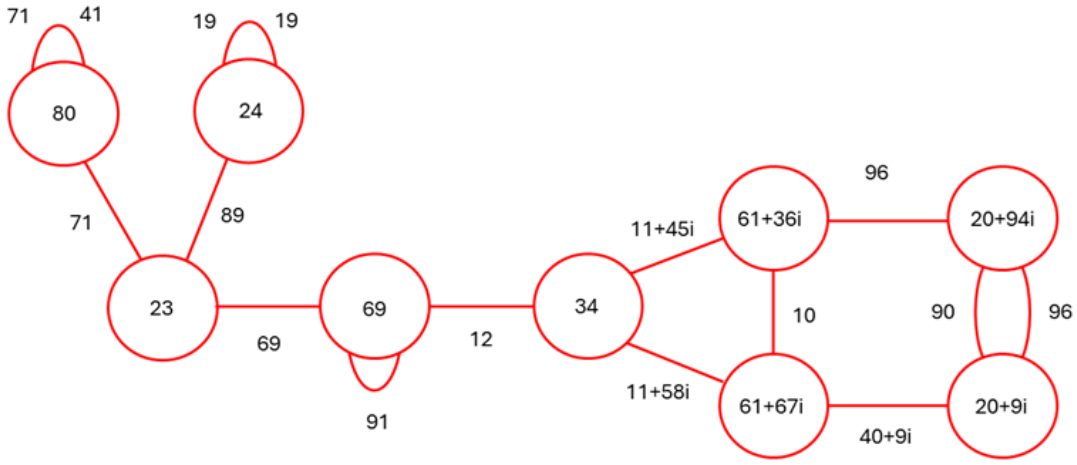

FIGURE 4. Supersingular 2-isogeny graph for $p = 103$.

10. CYCLES IN THE 2-ISOGENY GRAPH

We define a j-cycle of length N in the supersingular isogeny graph as a sequence

$$j_1,\ j_2, \ldots j_N\ , j_{N+1}$$

such that $j_1 = j_{N+1}$, and all j_k are different. Note that the latter condition does not permit to have an isogeny followed by the dual isogeny (backtracking), so the cycle lies in the isogeny graph. Also we do not allow to have a cycle of some length repeated a number of times, in particular we do not allow a self loop. Finally, in the case that there are two edges joining j_k and j_{k+1} (a double edge), we do not distinguish between the two isogenies involved.

There is recent interest on the study of cycles in the isogeny graph [1, 3, 9].

Theorem 10.1. *Given a j-cycle (j_n) of length N which does not include a double edge, there is a unique sequence $v_1, v_2, \ldots, v_N$, v_{N+1} such that $v_1 = v_{N+1}$, $j(v_n) = j_{n+1}$ and (v_n) satisfies (23). We call (v_n) the v-cycle associated to the j-cycle.*

Proof. The sequence (v_n) must satisfy:

$$v_{n+1}^2 = \frac{1}{2}\left(v_n + \frac{1}{v_n}\right), \tag{31}$$

$$j_{n+1} = 256\frac{(v_n^8 - v_n^4 + 1)^3}{(v_n^8 - v_n^4)^2}. \tag{32}$$

Let $\mu_n = v_n^4$, we see firstly that three consecutive values of μ_n determine a value of v_n, and then that three consecutive values of j_n determine a value of μ_n. The result follows from this.

Equations (22) and (31) are $4u_n u_{n+1}^2 = (u_n + 1)^2$, $2v_n v_{n+1}^2 = v_n^2 + 1$, where $\mu_n = u_n^2$, $u_n = v_n^2$. That is,

$$v_n = \frac{u_n + 1}{2u_{n+1}}$$

and

$$4\mu_{n+1} = \frac{(u_n + 1)^2}{u_n} = 2 + \frac{u_n^2 + 1}{u_n} = 2 + \frac{\mu_n + 1}{u_n},$$

from where

$$u_n = \frac{\mu_n + 1}{4\mu_{n+1} - 2}.$$

From here,

$$v_n = \frac{u_n + 1}{2u_{n+1}} = \frac{\dfrac{\mu_n + 1}{4\mu_{n+1} - 2} + 1}{2\dfrac{\mu_{n+1} + 1}{4\mu_{n+2} - 2}} = \frac{(\mu_n + 4\mu_{n+1} - 1)(2\mu_{n+2} - 1)}{2(2\mu_{n+1} - 1)(\mu_{n+1} + 1)}.$$

The cases $\mu_{n+1} \neq -1, \frac{1}{2}$ correspond to values $j_{n+2} = 1728$, which should be considered. In this case there is a self loop or a backtracking, cases which have been removed in our statement.

Next, we want to follow a similar approach to prove that three consecutive values j_n, j_{n+1}, j_{n+2} determine only one possible value of μ_n. The conditions we impose are:

$$\begin{aligned}
&j_n(\mu_{n-1}^2-\mu_{n-1})^2-256\,(\mu_{n-1}^2-\mu_{n-1}+1)=0,\\
&j_{n+1}(\mu_n^2-\mu_n)^2-256\,(\mu_n^2-\mu_n+1)=0,\\
&j_{n+2}(\mu_{n+1}^2-\mu_{n+1})^2-256\,(\mu_{n+1}^2-\mu_{n+1}+1)=0,\\
&4(2\mu_n-1)^2\mu_{n-1}-(\mu_{n-1}+1)^2=0,\\
&4(2\mu_{n+1}-1)^2\mu_n-(\mu_n+1)^2=0.
\end{aligned}$$

These are equation (32) for j_n, and (21) for μ_n.

From here we obtain an expression of μ_n that only depends on j_n, j_{n+1}, j_{n+2}. As this analysis is too complex for manual resolution, one follows a computational approach. One defines the ideal generated by these five polynomials and calculate a Groebner basis in the lexicographical order $(\mu_{n+1}, \mu_{n-1}, \mu_n, j_n, j_{n+2}, j_{n+1})$. Using a mathematical package as **Singular**, one obtains generators for this ideal. The first two generators are

$$\begin{aligned}
&(j_n-A)^3+(j_{n+1}-A)^3-j_n^2j_{n+1}^2+j_nj_{n+1}(Bj_n+Bj_{n+1}+C)+A^3=0,\\
&(j_{n+1}-A)^3+(j_{n+2}-A)^3-j_{n+1}^2j_{n+2}^2+j_{n+1}j_{n+2}(Bj_{n+1}+Bj_{n+2}+C)+A^3=0,
\end{aligned}$$

where $A=54000$, $B=1488$, $C=40773375$. These are the equations $\Phi_2(j_n, j_{n+1})=0$ and $\Phi_2(j_{n+1}, j_{n+2})=0$, using (28).

The third generator is

$$\begin{aligned}
\mu_n(16j_{n+1})(j_{n+1}+3375)(j_{n+1}^2+191025j_{n+1}-121287375)=\\
=j_{n+2}j_n^2+512j_{n+2}j_{n+1}j_n-108000j_{n+2}j_n+16j_{n+2}j_{n+1}^2+2757375j_{n+2}j_{n+1}\\
+2916000000j_{n+2}+256j_n^2j_{n+1}-54000j_n^2-256j_nj_{n+1}^3+434192j_nj_{n+1}^2\\
-140832000j_nj_{n+1}+5832000000j_n+188416j_{n+1}^3+4779648000j_{n+1}^2\\
-1332976500000j_{n+1}-157464000000000.
\end{aligned}$$

This gives a well defined value of μ_n if we assume that $j_{n+1}\neq 0, -3375$ and $j_{n+1}^2+191025j_{n+1}-121287375\neq 0$.

As we have seen in section 9, the value $j=0$ (respectively $j=-3375$) presents a self loop and the only way for a path to reach it is by passing twice through its adyacent node $j=287496$ (respectively $j=16581375$), which is not allowed in our definition of j-cycle as nodes may not be repeated. The condition $j_{n+1}^2+191025j_{n+1}-121287375=0$, on the other hand, only happens when the j-cycle traverses a double edge. This is an exceptional situation where there is more than one solution for the associated v-cycle,

reflecting the fact that there are actually two distinct edges that the j-cycle may follow. These cases has been ruled out in our statement. □

To finalize, we want to analyse further structure on the v-cycles. For this, we use two transformations. The first one is the Galois automorphism $\sigma(v) = \overline{v}$ defined as conjugation on $\mathbb{F}_{p^2} = \mathbb{F}_p[\mathbf{i}]$, that is, $\sigma(a + b\,\mathbf{i}) = a - b\,\mathbf{i}$. This is a field automorphism. Therefore, for a v-cycle $v_1, \ldots, v_N$, we have that

$$\sigma(v_{k+1})^2 = \frac{1}{2}\left(\sigma(v_k) + \frac{1}{\sigma(v_k)}\right),$$

and hence $\sigma(v_1), \ldots, \sigma(v_N)$ is a v-cycle, and the corresponding j-cycle is given by the Galois conjugates of $j_1, \ldots, j_N$.

The second transformation is the Moebius map

$$T(v) = \frac{v+1}{v-1}.$$

Note that $T(0) = -1$, $T(-1) = 0$, $T(\infty) = 1$, $T(1) = \infty$. Therefore $T^2 = \mathrm{id}$. If $w^2 = \frac{1}{2}\left(v + \frac{1}{v}\right)$, then

$$\frac{1}{2}\left(T(w) + \frac{1}{T(w)}\right) = \frac{1}{2}\left(\frac{w+1}{w-1} + \frac{w-1}{w+1}\right) = \frac{w^2+1}{w^2-1} = \\ = \frac{\frac{1}{2}(v+\frac{1}{v})+1}{\frac{1}{2}(v+\frac{1}{v})-1} = \frac{v^2+2v+1}{v^2-2v+1} = \frac{(v+1)^2}{(v-1)^2} = T(v)^2,$$

that is $\{T(w), T(v)\}$ form a pair satisfying the recurrence (23). So if $\{v_1, v_2, \ldots, v_N\}$ is a v-cycle, then

$$\{T(v_N), \ldots, T(v_2), T(v_1)\}$$

is a v-cycle of the same length. The T-transform of this cycle is again $\{v_1, \ldots, v_N\}$.

Now we define, for a v-cycle $\mathbf{v} = \{v_1, \ldots, v_N\}$, the product

$$\omega_{\mathbf{v}} = \prod_{i=1}^{N} v_i$$

We have the following striking conjecture, that we have checked for values of N up to 11 (we have checked over the rationals, hence it is true for any p).

Conjecture 10.2. *The values $\omega_{\mathbf{v}}$ always satisfy the equations*

$$\prod_{k=1}^{k_M} \left(2^N\omega^2 + (-1)^k(2k-1)\omega + 1\right) = 0, \tag{33}$$

where the maximum value k_M is the nearest integer to $\sqrt{2}^N$. The number of N-cycles is thus $2k_M$.

The v-cycles should have products $\omega_{\mathbf{V}}$ the roots of (33).

Note that these are conjugate numbers, and the product is $\frac{1}{2^N}$, that is

$$\omega_{\mathbf{v}} = \frac{1}{2^{N+1}} \left((-1)^{k+1}(2k-1) \pm \sqrt{(2k-1)^2 - 2^{N+2}} \right),$$

and each value corresponds to a v-cycle. If the number $\omega_{\mathbf{v}} \notin \mathbb{F}_p$, that is the square root is imaginary, then the two roots are conjugate. If $\mathbf{v}$ is the v-cycle then

$$\omega_{\sigma(\mathbf{v})} = \overline{\omega_{\mathbf{v}}}$$

is the conjugate of the product for $\mathbf{v}$. Therefore, this produces the conjugate ω. Note that in this case $N(\omega) = \dfrac{1}{2^N}$.

If $\omega_{\mathbf{v}} \in \mathbb{F}_p$, then the other root of the quadratic equation is

$$\omega = \frac{1}{2^N \omega_{\mathbf{v}}} \in \mathbb{F}_p \,.$$

This appears as follows.

Proposition 10.3. *For the reversed cycle $T(\mathbf{v})^\dagger$, we have*

$$\omega_{\mathbf{v}}\, \omega_{T(\mathbf{v})^\dagger} = \frac{1}{2^N} \,.$$

Proof. We compute

$$\begin{aligned} \omega_{T(\mathbf{v})^\dagger} = \prod_{i=1}^{N} T(v_i) = \prod_{i=1}^{N} \frac{v_i + 1}{v_i - 1} = \prod_{i=1}^{N} \frac{v_i^2 - 1}{(v_i - 1)^2} = \\ = \prod_{i=1}^{N} \frac{\frac{1}{2}\left(v_{i-1} + \frac{1}{v_{i-1}} \right) - 1}{(v_i - 1)^2} = \prod_{i=1}^{N} \frac{\frac{1}{2v_{i-1}} (v_{i-1} - 1)^2}{(v_i - 1)^2} = \\ = \prod_{i=1}^{N} \frac{1}{2v_{i-1}} = \frac{1}{2^N} \frac{1}{\omega_{\mathbf{v}}} \,, \end{aligned}$$

using the cyclicity of $\mathbf{v}$. □

Acknowledgements. This research has been conducted as part of GMV's Project "Solución de Identidad Autosoberana", and carried out under an Artículo 60 contract at Universidad Carlos III de Madrid, with partial co-financing from the Spanish National Cybersecurity Institute (INCIBE) using resources from the Spanish "Plan de Recuperación, Transformación y Resiliencia", originating from the European Union's Recovery and Resilience Facility. The opinions expressed in this publication are those of the author(s) and do not necessarily reflect those of the co-financing entity.

Our warmest thanks to María Isabel González-Vasco who is the promoter of this work, put the two authors in contact as PI of the node UC3M of the above mentioned research project, and has carefully read the manuscript and gave us very useful comments.

References

[1] S. Arpin, R. Bowden, J. Clements, W. Ghantous, J. T. LeGrow, and K. Maughan. Cycles and cuts in supersingular l-isogeny graphs. Cryptology ePrint Archive, Paper 2025/155, 2025.

[2] S. Arpin, C. Camacho-Navarro, K. Lauter, J. Lim, K. Nelson, T. Scholl, and J. Sotáková. Adventures in supersingularland. *Experimental Mathematics*, 32(2):241–268, 2021.

[3] S. Arpin, M. Chen, K. E. Lauter, R. Scheidler, K. E. Stange, and H. T. N. Tran. *Orientations and Cycles in Supersingular Isogeny Graphs*, pages 25–86. Springer International Publishing, Cham, 2024.

[4] W. Beullens, L. D. Feo, S. D. Galbraith, and C. Petit. Proving knowledge of isogenies: a survey. *Des. Codes Cryptogr.*, 91(11):3425–3456, 2023.

[5] I. Connell. Elliptic curve handbook, 1999. `http://www.math.mcgill.ca/connell`.

[6] D. A. Cox. The arithmetic-geometric mean of gauss. *Enseignement Mathématique (2)*, 30:275–330, 1984.

[7] L. E. Dickson. Criteria for the irreducibility of functions in a finite field. *Bulletin of the American Mathematical Society*, 13:1–8, 1906.

[8] K. Eisenträger, S. Hallgren, K. E. Lauter, T. Morrison, and C. Petit. Supersingular isogeny graphs and endomorphism rings: Reductions and solutions. In J. B. Nielsen and V. Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part III*, volume 10822 of *Lecture Notes in Computer Science*, pages 329–368. Springer, 2018.

[9] W. Ghantous. Loops, multi-edges and collisions in supersingular isogeny graphs. *Advances in Mathematics of Communications*, 18(4):935–955, 2024.

[10] M. J. Griffin, K. Ono, N. Saikia, and W.-L. Tsai. Agm and jellyfish swarms of elliptic curves. *American Mathematical Monthly*, 130:355–369, 2023.

[11] Y. Hasegawa. Ш-curves over quadratic fields. *Manuscripta Mathematica*, 94(1):347–364, 1997.

[12] K. Kinjo and Y. Miyasaka. 2-adic arithmetic-geometric mean and elliptic curves. *Interdisciplinary Information Sciences*, 16:5–15, 2010.

[13] D. Kohel, K. Lauter, C. Petit, and J.-P. Tignol. On the quaternion isogeny path problem. *LMS Journal of Computation and Mathematics*, 17(A):418–432, 2014.

[14] D. R. Kohel. *Endomorphism Rings of Elliptic Curves Over Finite Fields*. PhD thesis, University of California, Berkeley, US, 1996.
[15] M. Mamah. The supersingular isogeny path and endomorphism ring problems: Unconditional reductions. Cryptology ePrint Archive, Paper 2024/1569, 2024.
[16] D. Robert. On the efficient representation of isogenies (a survey). *IACR Cryptol. ePrint Arch.*, page 1071, 2024.
[17] D. Shumow. Isogenies of elliptic curves: A computational approach, 2009.
[18] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate texts in mathematics*. Springer, 1986.
[19] J. Vélu. Isogénies entre courbes elliptiques. *Comptes Rendus de l'Académie des Sciences de Paris, Série A*, 273:238–241, 1971.
[20] L. C. Washington. *Elliptic curves: number theory and cryptography*, volume 50 of *Discrete Mathematics and Its Applications*. CRC Press, 2nd edition, 2008.
[21] B. Wesolowski. The supersingular isogeny path and endomorphism ring problems are equivalent. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1100–1111, 2022.

GMV, C/ Santiago Grisolía, 4, P.T.M. 28760 Tres Cantos, Madrid, Spain

Email address: jjleon@gmv.com

Departamento de Algebra, Geometría y Topología, Universidad Complutense de Madrid, Ciudad Universitaria 28040 Madrid, Spain

Email address: vicente.munoz@ucm.es