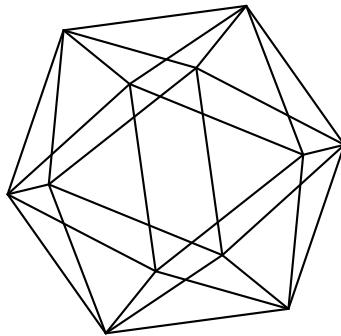# Max-Planck-Institut für Mathematik Bonn

Elliptic curves over Hasse pairs

by

Eleni Agathocleous
Antoine Joux
Daniele Taufer

Elliptic curves over Hasse pairs

by

Eleni Agathocleous
Antoine Joux
Daniele Taufer

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

CISPA Helmholtz Center for
Information Security
Stuhlsatzenhaus 5
66123 Saarbrücken
Germany

KU Leuven
Celestijnenlaan 200 A - Box 2402
3001 Leuven
Belgium

ELLIPTIC CURVES OVER HASSE PAIRS

ELENI AGATHOCLEOUS, ANTOINE JOUX, AND DANIELE TAUFER

with an appendix by
PIETER MOREE AND EFTHYMIOS SOFOS

ABSTRACT. We call a pair of distinct prime powers $(q_1, q_2) = (p_1^{a_1}, p_2^{a_2})$ a Hasse pair if $|\sqrt{q_1} - \sqrt{q_2}| \leq 1$. For such pairs, we study the relation between the set $\mathcal{E}_1$ of isomorphism classes of elliptic curves defined over $\mathbb{F}_{q_1}$ with q_2 points, and the set $\mathcal{E}_2$ of isomorphism classes of elliptic curves over $\mathbb{F}_{q_2}$ with q_1 points. When both families $\mathcal{E}_i$ contain only ordinary elliptic curves, we prove that their isogeny graphs are isomorphic. When supersingular curves are involved, we describe which curves might belong to these sets. We also show that if both the q_i's are odd and $\mathcal{E}_1 \cup \mathcal{E}_2 \neq \emptyset$, then $\mathcal{E}_1 \cup \mathcal{E}_2$ always contains an ordinary elliptic curve. Conversely, if q_1 is even, then $\mathcal{E}_1 \cup \mathcal{E}_2$ may contain only supersingular curves precisely when q_2 is a given power of a Fermat or a Mersenne prime. In the case of odd Hasse pairs, we could not rule out the possibility of an empty union $\mathcal{E}_1 \cup \mathcal{E}_2$, but we give necessary conditions for such a case to exist. In an appendix, Moree and Sofos consider how frequently Hasse pairs occur using analytic number theory, making a connection with Andrica's conjecture on the difference between consecutive primes.

1. INTRODUCTION

Given an elliptic curve E over a finite field $\mathbb{F}_q$ of characteristic p, its number of points $|E(\mathbb{F}_q)|$ is directly related with a number t, called the trace of $E/\mathbb{F}_q$, which is defined as

$$t = q + 1 - |E(\mathbb{F}_q)|.$$

All elliptic curves over $\mathbb{F}_q$ with the same number of rational points have the same trace, which we will denote by t. We can then consider the set $\mathcal{E}(t)$ of $\mathbb{F}_q$-isomorphism classes of elliptic curves $E/\mathbb{F}_q$ with trace t:

$$\mathcal{E}(t) = \{E/\mathbb{F}_q \ : \ |E(\mathbb{F}_q)| = q + 1 - t\}/\{\mathbb{F}_q\text{-isomorphisms}\}.$$

It is of both mathematical and cryptographic interest, to study such families $\mathcal{E}(t)$ over some finite field $\mathbb{F}_q$, when the number of points, and therefore the trace t, is given. In this paper, we are interested in a 'dual formulation' of this problem: given two prime powers q_1, q_2, we investigate the two sets

$$\mathcal{E}_1 = \{E_1/\mathbb{F}_{q_1} \ : \ |E_1(\mathbb{F}_{q_1})| = q_2\}/\{\mathbb{F}_{q_1}\text{-isomorphisms}\},$$

and

$$\mathcal{E}_2 = \{E_2/\mathbb{F}_{q_2} \ : \ |E_2(\mathbb{F}_{q_2})| = q_1\}/\{\mathbb{F}_{q_2}\text{-isomorphisms}\}.$$

To exclude trivial cases, we further ask that the two prime powers q_1, q_2 be different and satisfy the relation

$$|\sqrt{q_1} - \sqrt{q_2}| \leq 1.$$

When this relation holds true, we call such a pair (q_1, q_2) a *Hasse pair*. We remark that the case $|\sqrt{q_1} - \sqrt{q_2}| > 1$ is degenerate: when q_1, q_2 do not belong to the Hasse interval of each other, then both sets $\mathcal{E}_i$ are necessarily empty.

The integer $t_1 = q_1 + 1 - q_2$ (resp. $t_2 = q_2 + 1 - q_1$) will be referred to as the trace of $\mathcal{E}_1$ (resp. $\mathcal{E}_2$), as it equals the trace of every curve (if any) in the corresponding set.

When $E_1 \in \mathcal{E}_1$ and $E_2 \in \mathcal{E}_2$ both arise as good reductions of a global curve E, the pair (q_1, q_2) was called *amicable* or 2-*aliquot cycle* for E [7, 31], and the distribution of amicable primes for a given E was notably shown to depend on whether E has complex multiplication [16, 25, 31]. If the E_i's share the same endomorphism ring $\mathcal{O}$, the pair (q_1, q_2) has been referred to as *dual elliptic* associated to $\mathcal{O}$ [21]. In cryptography, such pairs of curves (E_1, E_2) are called *2-cycles*, and may be employed to design recursive zk-SNARK protocols [5]. Those are particularly efficient when the considered curves are pairing-friendly, which poses strong constraints on the feasible curves [4, 9]. Examples of such applications appeared, among others, in [6, 14, 15, 20], and we refer the interested reader to [2] for an extensive survey on this topic.

1.1. **Novel contributions.** Unlike previous related works, in this paper we do not start from a global curve. We observe instead that for a given Hasse pair, the associated traces t_i are linearly dependent (Remark 3.2) and they have the same discriminant Δ (Lemma 3.5), which prescribes whether the corresponding elliptic curves are ordinary or supersingular (Lemma 3.10). Furthermore, even though the set $\mathcal{E}_i$ may occasionally be empty, even when (q_1, q_2) is a Hasse pair, this never occurs when the q_i's are pure primes (Lemma 3.11); and in this case, both sets $\mathcal{E}_i$ consist of ordinary elliptic curves, except for a few small exceptions (Remark 3.12).

For every choice of odd Hasse pair $(p_1^{a_1}, p_2^{a_2})$, at least one of the p_i's is proved to split completely in $\mathbb{Q}(\sqrt{\Delta})$ (Proposition 5.6).

For any Hasse pair (q_1, q_2), both the sets $\mathcal{E}_i$ are likely to consist of ordinary elliptic curves, and in this case, the directed multigraphs of their prime degree $\mathbb{F}_{q_i}$-isogenies are isomorphic (Theorem 6.9). However, special choices of the q_i's may lead to different configurations. When both the q_i's are odd, at most one of the sets $\mathcal{E}_i$ may contain supersingular elliptic curves (Proposition 4.2), while this fails with even characteristic in a specific list of cases involving Fermat and Mersenne primes (Theorem 4.6). Moreover, if q_1 is even, then the existence of a curve in $\mathcal{E}_1$ is sufficient to guarantee that $\mathcal{E}_2$ is also non-empty (Lemma 4.4 and Theorem 4.6).

The only open case left is $\mathcal{E}_1 \cup \mathcal{E}_2 = \emptyset$. In even characteristic this can happen, but we found only one such instance, namely $(q_1, q_2) = (2^8, 3^5)$. We did not find any such a pair when both the q_i's are odd, and we proved that such an example (if existent) should satisfy strict numerical conditions (Proposition 5.11).

Problem 1.1. *Characterizing Hasse pairs (q_1, q_2) such that $\mathcal{E}_1$ and $\mathcal{E}_2$ are both empty. In particular, deciding if the set of such pairs is finite (or even empty, in odd characteristics).*

To the best of our knowledge, Problem 1.1 is open, except for cases of very small exponents ruled out by Corollary 5.12. The possible configurations of sets $\mathcal{E}_i$ discussed in the present paper are displayed by Tables 1 and 2.

Finally, given the interesting properties that these sets of elliptic curves and their graphs exhibit, it is natural to ask, not only out of mathematical curiosity but also from a cryptographic perspective, whether there are many Hasse pairs. This question is directly related to

a long-standing conjecture known as Andrica's conjecture, which states that the difference of the square roots of any two consecutive primes is always less than one. In Appendix A, Moree and Sofos discuss this conjecture in the context of prime powers, and they prove an asymptotic result regarding the number of Hasse pairs in which a given prime p can be a member.

1.2. **Notation.** We denote the set of natural numbers by $\mathbb{N} = \{0, 1, \dots\}$, and its positive subset by $\mathbb{Z}_{>0} = \{1, 2, \dots\}$. We write $p^a || N$ when $p^a | N$ but $p^{a+1} \nmid N$. When the order of the elements of a pair is irrelevant, we denote it by $((q_1, q_2))$ to indicate (q_1, q_2) or (q_2, q_1).

1.3. **Paper organization.** In Section 2 we recall a theorem of Waterhouse on valid traces, and we prove a corollary of this result regarding elliptic curves of j-invariant zero. In Section 3, we define Hasse pairs and we establish several properties of its associated discriminant Δ and traces t_1 and t_2. In Section 4 we focus on the non-ordinary cases, i.e. when at least one of the sets $\mathcal{E}_1$ or $\mathcal{E}_2$ is empty or is comprised of supersingular elliptic curves. Section 5 is devoted to the splitting behavior of the base primes of a given Hasse pair in the corresponding imaginary quadratic field $\mathbb{Q}(\sqrt{\Delta})$. In Section 6, we deal with the ordinary case and we establish the correspondence between the isogeny graphs of the elliptic curves in $\mathcal{E}_1$ and of those in $\mathcal{E}_2$. Some numerical and visual examples of such graphs are presented in Section 7. Finally, in Section 8, we summarise the results of the current paper, and we draw our conclusions.

2. Valid Traces

Let $q \in \mathbb{Z}_{>0}$ be a prime power. We consider all elliptic curves over $\mathbb{F}_q$ with the same number of points or, equivalently, with the same trace $t \in \mathbb{Z}$. We denote the set of $\mathbb{F}_q$-isomorphism classes of such curves by $\mathcal{E}(t)$. The following theorem of Waterhouse determines when $\mathcal{E}(t)$ is not empty and the type of elliptic curves it contains.

Theorem 2.1 ([35, Theorem 4.1]). *Let $\mathcal{E}(t)$ be the set of elliptic curves of trace t over $\mathbb{F}_q = \mathbb{F}_{p^a}$. Then $\mathcal{E}(t)$ is non-empty precisely in the following cases.*

(a) $|t| \leq 2\sqrt{q}$, with $\gcd(t, q) = 1$.
(b) $t = \pm 2\sqrt{q}$, and a is even.
(c) $t = \pm\sqrt{q}$, with $p \not\equiv 1 \bmod 3$ and a is even.
(d) $t = \pm\sqrt{p^{a+1}}$, with $p \in \{2, 3\}$ and a is odd.
(e) $t = 0$, and (I) a is odd or (II) a is even, and $p \not\equiv 1 \bmod 4$.

The elliptic curves of case (a) are ordinary. The curves of case (b) are supersingular and have all their endomorphisms defined over $\mathbb{F}_q$, while the rest are supersingular but do not have all their endomorphisms defined over $\mathbb{F}_q$.

By [35, Theorems 4.1 and 4.2], one can deduce the values of the j-invariants for some of the cases of Theorem 2.1. Since we have not found this result in the literature, we state and prove it here, for completeness.

Proposition 2.2. *The elliptic curves corresponding to cases (c) and (d) in Theorem 2.1 have j-invariant 0.*

Proof. Since the CM-discriminant is $\Delta = t^2 - 4q$, we have

$$t = \begin{cases} \pm p^{\frac{a}{2}} & \text{with } a \text{ even,} \\ \pm p^{\frac{a+1}{2}} & \text{with } p \in \{2,3\}, a \text{ odd.} \end{cases} \implies \Delta = \begin{cases} -3q & \text{in case (c),} \\ (p-4)q & \text{in case (d).} \end{cases}$$

The elliptic curves corresponding to the above cases, do not have all their endomorphisms defined over $\mathbb{F}_q$, hence by [35, Theorem 4.2-(3)] the possible endomorphism rings arising from the elliptic curves in $\mathcal{E}(t)$ have conductor coprime to q.

In case (c) the possible conductors are those dividing $\sqrt{q}$, therefore the unique possible order is the maximal one, i.e. the ring of integers of $\mathbb{Q}(\sqrt{-3})$, which is the endomorphism ring of curves with j-invariant 0.

Similarly, in case (d), if $p = 2$ the possible conductors are those dividing $2^{(a+1)/2}$, therefore the unique possible order is the ring of integers of $\mathbb{Q}(i)$, which is defined by curves with j-invariant $1728 = 0 \in \mathbb{F}_q$. If $p = 3$ the conductors need to divide $3^{(a-1)/2}$, therefore the unique endomorphism order is the ring of integers of $\mathbb{Q}(\sqrt{-3})$, which is again defined by curves with j-invariant 0. $\qquad\square$

3. Hasse pairs

Throughout the paper, $q_1 = p_1^{a_1}$ and $q_2 = p_2^{a_2}$ will denote arbitrary prime powers. Given such a pair (q_1, q_2), we consider the (possibly empty) set of elliptic curves defined over $\mathbb{F}_{q_1}$ with q_2 rational points, and respectively the set of elliptic curves over $\mathbb{F}_{q_2}$ with q_1 points. To avoid trivial repetitions, we consider these curves up to $\mathbb{F}_{q_i}$-isomorphism.

Definition 3.1. *Let (q_1, q_2) be a pair of distinct prime powers. For $(i,j) = ((1,2))$, we define*

$$\mathcal{E}_i = \{E_i/\mathbb{F}_{q_i} : |E_i(\mathbb{F}_{q_i})| = q_j\}/\{\mathbb{F}_{q_i}\text{-isomorphisms}\}.$$

We also define the trace t_i *corresponding to such a pair as*

$$t_i = q_i + 1 - q_j.$$

Remark 3.2. *The integers t_i are the traces of the Frobenius morphism for every elliptic curve (if any) in $\mathcal{E}_i$ [30, Remark V.2.6]. Moreover, by adding their defining equations, we immediately see that*

$$t_1 + t_2 = 2.$$

Remark 3.3. *The results of the present paper would hold even when $q_1 = q_2$. We have excluded this case from Definition 3.1, since it leads to the trivial relations $\mathcal{E}_1 = \mathcal{E}_2$ and $t_1 = t_2 = 1$. These curves of trace 1 are often called* anomalous *curves, and are all ordinary by Theorem 2.1 (a).*

Definition 3.4. *We define the* discriminant *associated with the pair (q_1, q_2) as*

$$\Delta = (q_1 - q_2)^2 - 2(q_1 + q_2) + 1.$$

As we prove below, this is the maximal CM-discriminant of the curves in the sets $\mathcal{E}_i$, when they are not empty. An analogous result for amicable curves was already observed in [31, Proposition 3.4].

Lemma 3.5. *Let t_1, t_2 and Δ be defined as above. Then*

$$t_1^2 - 4q_1 = \Delta = t_2^2 - 4q_2.$$

Proof. By the definition of t_1 we have

$$t_1^2 - 4q_1 = (q_1 - q_2)^2 + 2(q_1 - q_2) + 1 - 4q_1 = \Delta,$$

which is symmetric in q_1 and q_2, thus it also equals $t_2^2 - 4q_2$. $\qquad\square$

Hasse's Theorem [30, Theorem V.1.1] implies that the sets $\mathcal{E}_i$ can be non-empty if the considered q_i's are close enough. This motivates the following definition.

Definition 3.6 (Hasse pair)**.** *Let q_1, q_2 be distinct prime powers. We call the pair (q_1, q_2) a Hasse pair iff*

$$|\sqrt{q_1} - \sqrt{q_2}| \leq 1.$$

When both q_1 and q_2 are odd, we will refer to it as an odd Hasse pair.

The following lemma links the above definition to Hasse's theorem.

Lemma 3.7. *Let t_1, t_2 be defined as above. The following are equivalent:*

(1) (q_1, q_2) is a Hasse pair,
(2) $|t_1| \leq 2\sqrt{q_1}$,
(3) $|t_2| \leq 2\sqrt{q_2}$.

Proof. Condition (1) is equivalent to

$$\sqrt{q_2} - 1 \leq \sqrt{q_1} \leq \sqrt{q_2} + 1.$$

Since all the quantities are positive, this is equivalent to its squared version, namely

$$q_2 - 2\sqrt{q_2} + 1 \leq q_1 \leq q_2 + 2\sqrt{q_2} + 1.$$

This can be written as

$$-2\sqrt{q_2} \leq -(q_2 - q_1 + 1) \leq 2\sqrt{q_2},$$

which is condition (3). Since condition (1) is symmetric, the equivalence between (1) and (2) follows in the same way, by reversing the roles of q_1 and q_2. $\qquad\square$

An elliptic curve over $\mathbb{F}_{q_i}$ is called *supersingular* if its trace is divisible by p_i, and *ordinary* otherwise. Since all the curves in $\mathcal{E}_i$ (if any) have the same trace t_i, then the set $\mathcal{E}_i$ is either empty or contains curves that have the same type (i.e. they are all ordinary or all supersingular). This motivates the following definition.

Definition 3.8. *We call the set $\mathcal{E}_i$ ordinary (resp. supersingular) if it is non-empty and contains ordinary (resp. supersingular) elliptic curves.*

Remark 3.9. *We recall that two ordinary curves are isomorphic over $\mathbb{F}_q$ if and only if they have the same size and the same j-invariant [10, Proposition 14.19]. Hence, when the set $\mathcal{E}_i$ is ordinary, it can be identified with the set containing the j-invariants of all elliptic curves that belong to $\mathcal{E}_i$.*

Lemma 3.10. *Let (q_1, q_2) be a Hasse pair. For both $i \in \{1, 2\}$, the following hold.*

- *If $\gcd(\Delta, q_i) = 1$, then $\mathcal{E}_i$ is ordinary.*
- *If $\gcd(\Delta, q_i) \neq 1$, then $\mathcal{E}_i$ is either supersingular or empty.*

Proof. We notice that

$$\gcd(t_i, q_i) = 1 \iff \gcd(t_i^2 - 4q_i, q_i) = 1 \iff \gcd(\Delta, q_i) = 1.$$

All the curves of $\mathcal{E}_i$ (if any) have trace t_i (Remark 3.2), hence they are ordinary when $\gcd(\Delta, q_i) = 1$, and supersingular when $\gcd(\Delta, q_i) \neq 1$. Since $|t_i| \leq 2\sqrt{q_i}$ by Lemma 3.7, in the ordinary case the set $\mathcal{E}_i$ is always non-empty (see Theorem 2.1, case (a)). $\square$

When dealing with pure primes, the sets $\mathcal{E}_i$ are almost always comprised of ordinary curves, as shown by the next lemma.

Lemma 3.11. *If (p_1, q_2) is a Hasse pair, with p_1 prime, then $\mathcal{E}_1$ is non-empty. Moreover, if $\mathcal{E}_1$ is supersingular then $q_2 = p_1 + 1$ or $p_1 \in \{2, 3\}$.*

Proof. Since (q_1, q_2) is Hasse, by Lemma 3.7 we have $|t_1| \leq 2\sqrt{p_1} < 2p_1$. If $p_1 \in \{2, 3\}$, the integer values lying between $-2p_1$ and $2p_1$ are either coprime to p_1 (a), or equal to $\pm p_1$ (d), or equal to 0 (e).

When $p_1 > 3$, we have the tighter bound $|t_1| \leq 2\sqrt{p_1} < p_1$. In this case, the integers between $-p_1$ and p_1 are either coprime to p_1 (a) or equal to 0 (e). In all such cases, $\mathcal{E}_1$ is non-empty by Theorem 2.1. Furthermore, if $p_1 > 3$ the only supersingular case has $t_1 = 0$ which implies $q_2 = p_1 + 1$. $\square$

Remark 3.12. *As a consequence of Lemma 3.11, whenever (p_1, p_2) is a Hasse pair consisting of pure primes (i.e. $a_1 = a_2 = 1$), in all but a few small cases, both sets $\mathcal{E}_i$ are ordinary. A straightforward verification of those cases shows that $\mathcal{E}_1$ is actually supersingular precisely when $(p_1, p_2) \in \{(2,3), (2,5), (3,7)\}$.*

Example 3.13. *Since $\sqrt{7} - \sqrt{3} = 0.913\ldots$, then $(p_1, p_2) = (3, 7)$ is an odd Hasse pair. Up to isomorphism, there is only one elliptic curve in $\mathcal{E}_1$, defined by $y^2 = x^3 + 2x + 1$. As $t_1 = 3 + 1 - 7 = -3$, this curve is supersingular. Similarly, there is only one curve in $\mathcal{E}_2$, defined by $y^2 = x^3 + 4$. It has trace $t_2 = 2 - t_1 = 5$, hence it is ordinary. Finally, we notice that the j-invariant of both curves is 0, and this is not a coincidence as we show in Proposition 4.3.*

4. NON-ORDINARY CASES

In this section, we discuss the relation between $\mathcal{E}_1$ and $\mathcal{E}_2$ when $\gcd(\Delta, q_1 q_2) \neq 1$, namely when at least one of these sets is either supersingular or empty.

We begin by noticing that non-ordinary cases may occur only in different characteristics.

Lemma 4.1. *If $p_1 = p_2$, then $\gcd(\Delta, q_1 q_2) = 1$.*

Proof. If $p_1 = p_2$, then $q_i = p_1^{e_i}$. Therefore

$$\Delta = (q_1 - q_2)^2 - 2(q_1 + q_2) + 1 \equiv 1 \bmod p_1,$$

which implies $\gcd(\Delta, q_1 q_2) = 1$. $\square$

4.1. **Odd characteristics.** When q_1 and q_2 are both odd, then so are t_1 and t_2.

Proposition 4.2. *Let (q_1, q_2) be an odd Hasse pair. If $\mathcal{E}_1$ is supersingular, then $\mathcal{E}_2$ is ordinary. Thus, if $\mathcal{E}_1 \cup \mathcal{E}_2$ is non-empty, then it always contains an ordinary elliptic curve.*

Proof. Let $E_1 \in \mathcal{E}_1$ be a supersingular curve. We first consider the case $p_1 \neq 3$. Since t_1 is odd, only case (c) of Theorem 2.1 can apply. Thus, a_1 needs to be even and $t_1 = \pm\sqrt{q_1}$, hence $\Delta = t_1^2 - 4q_1 = -3q_1$. Since $\gcd(q_1, q_2) = 1$ by Lemma 4.1, then $\gcd(\Delta, q_2) \in \{1, 3\}$.

Let us assume by contradiction that $p_2 = 3$, then by Remark 3.2 we get

$$2 - t_1 = t_2 = 3^{a_2} + 1 - p_1^{a_1}, \quad \text{which implies} \quad p_1^{a_1} \mp p_1^{\frac{a_1}{2}} + 1 = 3^{a_2}.$$

If $a_2 = 1$, then $q_2 = 3$ and the only odd prime powers inside its Hasse interval are 5 and 7, both with odd exponents, contradicting the parity of a_1. If $a_2 > 1$, then $x = -p_1^{\frac{a_1}{2}}$ should be a root of one of the polynomials

$$x^2 \pm x + 1 \in \mathbb{Z}/9\mathbb{Z}[x],$$

which is impossible since those polynomials are both irreducible. Hence, we conclude that $p_2 \neq 3$, which implies $\gcd(\Delta, q_2) = 1$, then $\mathcal{E}_2$ is ordinary by Lemma 3.10.

Let us now consider the case $p_1 = 3$. Since t_1 is odd, by Theorem 2.1 we have

$$t_1 = \begin{cases} \pm 3^{\frac{a_1}{2}} & \text{if } a_1 \text{ is even,} \quad \text{case (c),} \\ \pm 3^{\frac{a_1+1}{2}} & \text{if } a_1 \text{ is odd,} \quad \text{case (d),} \end{cases}$$

which leads us to

$$\Delta = \begin{cases} (3^{\frac{a_1}{2}})^2 - 4 \cdot 3^{a_1} = -3^{a_1+1} & \text{if } a_1 \text{ is even,} \\ (3^{\frac{a_1+1}{2}})^2 - 4 \cdot 3^{a_1} = -3^{a_1} & \text{if } a_1 \text{ is odd.} \end{cases}$$

By Lemma 4.1 we have $\gcd(q_1, q_2) = 1$, therefore $3 \nmid q_2$. Hence, Δ and q_2 cannot have common factors and we conclude that $\mathcal{E}_2$ is ordinary by Lemma 3.10.

Thus, for odd Hasse pairs the sets $\mathcal{E}_i$ cannot be both supersingular, then if $\mathcal{E}_1 \cup \mathcal{E}_2$ is not empty, then it contains an ordinary elliptic curve. $\square$

Next, we show that in odd characteristics, establishing the existence of supersingular curves in $\mathcal{E}_1 \cup \mathcal{E}_2$ only requires testing curves with j-invariant 0.

Proposition 4.3. *Let (q_1, q_2) be an odd Hasse pair. If $E_1 \in \mathcal{E}_1$ is supersingular, then $j(E_1) = 0$. Furthermore, in this case $\mathcal{E}_2$ is ordinary and it also contains an elliptic curve with j-invariant 0.*

Proof. Since t_1 is odd, we are in cases (c) or (d) of Theorem 2.1, thus by Proposition 2.2 we have $j(E_1) = 0$. Moreover, by Proposition 4.2, $\mathcal{E}_2$ is ordinary and, by [35, Theorem 4.2 (2)], the maximal order always arises as the endomorphism ring of some curve in $\mathcal{E}_2$. We have

$$t_1 = \begin{cases} \pm p_1^{\frac{a_1}{2}} & \text{if } a_1 \text{ is even,} \\ \pm 3^{\frac{a_1+1}{2}} & \text{if } a_1 \text{ is odd,} \end{cases} \implies \Delta = \begin{cases} -3p_1^{a_1} & \text{if } a_1 \text{ is even,} \\ -3^{a_1} & \text{if } a_1 \text{ is odd.} \end{cases}$$

We observe that the maximal order in both cases is the ring of integers of $\mathbb{Q}(\sqrt{-3})$, which is always isomorphic to the endomorphism ring of elliptic curves of j-invariant 0. $\square$

4.2. **Even characteristics.** In this section, we discuss Hasse pairs involving even prime powers, so we will assume $p_1 = 2$.

Lemma 4.4. *Let $(2^{a_1}, q_2)$ be a Hasse pair. The following are equivalent:*

(1) $\mathcal{E}_1$ is ordinary,
(2) q_2 is even,
(3) $(2^{a_1}, q_2) \in \{((2, 4)), ((4, 8))\}$.

Proof. (1) $\Rightarrow$ (2): Since $\mathcal{E}_1$ is ordinary, then t_1 is odd, so is t_2 (Remark 3.2). Therefore $q_2 = t_2 - 1 + 2^{a_1}$ is even.

(2) $\Rightarrow$ (3): A straightforward check shows that there are only two powers of 2 lying in the Hasse bound of each other, namely $\{2, 4\}$ and $\{4, 8\}$.

(3) $\Rightarrow$ (1): Every $(2^{a_1}, q_2) \in \{((2, 4)), ((4, 8))\}$ has discriminant $\Delta = -7$, which is coprime to 2^{a_1}. Thus, $\mathcal{E}_1$ is ordinary by Lemma 3.10. $\qquad\square$

The ordinary cases of Lemma 4.4 are detailed in Examples 7.2 and 7.3. Except for such cases, if $\gcd(\Delta, q_1 q_2) \neq 1$ we can assume that q_2 is odd and $\mathcal{E}_1$ is supersingular or empty. In the supersingular case, we know from Deuring [12, §8.2] that the only possible curves in $\mathcal{E}_1$ have j-invariant 0, similarly to the odd case (Proposition 4.3).

However, with an even characteristic one may simultaneously find supersingular curves in both $\mathcal{E}_1$ and $\mathcal{E}_2$. To determine when this is the case we need the following lemma. It is an easy instance of the theorem of Mihăilescu [22], which proved the famous Catalan's conjecture, but the version we need can be proved with elementary techniques.

Lemma 4.5 ([28, pp. 201-203]). *Let $\alpha, \beta \geq 2$ be integers and let $p \in \mathbb{N}$ be a prime. If 2^α and p^β are consecutive integers, then $\alpha = 3, \beta = 2$ and $p = 3$.*

Theorem 4.6. *Let $(q_1, q_2) = (2^{a_1}, p_2^{a_2})$ be a Hasse pair. If $\mathcal{E}_1$ is supersingular of trace t_1, then precisely one of the following holds.*

(1) $t_1 = \pm 2^{\frac{a_1+2}{2}}$ and

$$(q_1, q_2) = \begin{cases} (2^6, 3^4), & \text{or} \\ (2^{2^{n+1}}, (2^{2^n} + 1)^2), & \text{with } p_2 = 2^{2^n} + 1 \text{ a Fermat prime, or} \\ (2^{2m}, (2^m - 1)^2), & \text{with } p_2 = 2^m - 1 \text{ a Mersenne prime.} \end{cases}$$

(2) $t_1 = 2$ and $(q_1, q_2) = (2^2, 3)$.

(3) $t_1 = 0$, or a_1 is odd and $t_1 = \pm 2^{\frac{a_1+1}{2}}$, or a_1 is even, $t_1 = \pm 2^{\frac{a_1}{2}}$ and $p_2 \neq 3$.

In cases (1) and (2), $\mathcal{E}_2$ is supersingular, while in case (3), $\mathcal{E}_2$ is ordinary.

Proof. Since $\mathcal{E}_1$ is supersingular, then p_2 is odd by Lemma 4.4 and t_1 is given by one of the cases (b)-(e) of Theorem 2.1. We examine such cases separately.

Case (b): a_1 is even and $t_1 = \pm 2^{\frac{a_1+2}{2}}$, thus $\Delta = t_1^2 - 4q_1 = 2^{a_1+2} - 4 \cdot 2^{a_1} = 0$. Since $\Delta = t_2^2 - 4p_2^{a_2}$ by Lemma 3.5, then a_2 is also even. As (q_1, q_2) is Hasse, this implies that $2^{\frac{a_1}{2}}$ and $p_2^{\frac{a_2}{2}}$ are consecutive integers. By Lemma 4.5 if $\frac{a_1}{2}, \frac{a_2}{2} \geq 2$ there is a unique possibility, namely $(q_1, q_2) = (2^6, 3^4)$, corresponding to the consecutive integers 8 and 9. Now consider the case where a_1 or a_2 is 2. If $a_1 = 2$, we straightforwardly verify that there are no Hasse pairs $(4, p_2^{a_2})$ with a_2 even. If $a_2 = 2$, then $2^{\frac{a_1}{2}}$ and p_2 are consecutive integers, therefore p_2 is either a Fermat or a Mersenne prime. It is easy to check that the corresponding traces t_2 fit into case (b) of Theorem 2.1, hence in such cases $\mathcal{E}_2$ is supersingular.

Case (c): a_1 is even and $t_1 = \pm 2^{\frac{a_1}{2}}$, then $\Delta = -3 \cdot 2^{a_1}$. If $p_2 > 3$ then $\mathcal{E}_2$ is ordinary by Lemma 3.10. Let us consider $p_2 = 3$. By Lemma 3.5 we have

$$-3 \cdot 2^{a_1} = t_2^2 - 4 \cdot 3^{a_2}.$$

Since -3 is not a quadratic residue modulo 9, the above equation may have integer solutions only if $a_2 = 1$, hence $q_2 = 3$. We straightforwardly check that the unique Hasse pair $(2^{a_1}, 3)$ with a_1 even is $(2^2, 3)$, which gives $t_1 = 2, t_2 = 0$ and therefore $\mathcal{E}_2$ supersingular.

Cases (d) and (e): If a_1 is odd and $t_1 = \pm 2^{\frac{a_1+1}{2}}$, or if $t_1 = 0$, then Δ is a power of 2, hence $\mathcal{E}_2$ is ordinary by Lemma 3.10. □

Remark 4.7. *By Proposition 4.3 and Theorem 4.6, both sets $\mathcal{E}_i$ can be simultaneously supersingular only if one of the considered prime powers is even, and the other one involves primes of Fermat or Mersenne. On the other side, if the Lenstra-Pomerance-Wagstaff conjecture [34] holds true, this would imply the existence of infinitely many Mersenne primes, hence by Theorem 4.6 both sets $\mathcal{E}_i$ are supersingular infinitely many times.*

Remark 4.8. *When both sets $\mathcal{E}_i$ are supersingular, they are often unrelated. For instance, for $(q_1, q_2) = (2^{10}, 31^2)$ the set $\mathcal{E}_1$ contains one curve of j-invariant $0 \in \mathbb{F}_{2^{10}}$, while $\mathcal{E}_2$ contains three curves of j-invariants $2, 4, 23 \in \mathbb{F}_{31^2}$. Instead, in the next sections we will prove that this is never the case when both sets $\mathcal{E}_i$ are ordinary.*

5. The splitting behavior of the primes in odd Hasse pairs

In this section, we consider odd Hasse pairs (q_1, q_2), and therefore the traces t_i are both odd integers.

Lemma 5.1. *Let (q_1, q_2) be an odd Hasse pair. Then $\Delta < 0$, $\Delta \equiv 1 \bmod 4$ and $|\Delta|$ is not a perfect square.*

Proof. Since (q_1, q_2) is Hasse and t_1 is odd, by Lemma 3.7 we have $t_1 < 2\sqrt{q_1}$, hence by Lemma 3.5 we conclude
$$\Delta = t_1^2 - 4q_1 < 0.$$
Since $t_1^2 \equiv 1 \bmod 4$, the above equation implies $\Delta \equiv 1 \bmod 4$, so $|\Delta| = -\Delta \equiv -1 \bmod 4$. Therefore $|\Delta|$ cannot be a square, as it is not a quadratic residue modulo 4. □

We can write the discriminant Δ associated with (q_1, q_2) as
$$\Delta = f^2 D,$$
where f is called the *conductor*, and D is the squarefree part of Δ. By Lemma 5.1, we have $D \equiv 1 \bmod 4$ as well, hence D is a fundamental discriminant. We denote by K the imaginary quadratic field
$$K = \mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{D}),$$
and by $\mathcal{O}_K$ the maximal order of K.

Remark 5.2. *When (q_1, q_2) is an odd Hasse pair, we observe that we never have $K = \mathbb{Q}(i)$, since $\Delta \equiv 1 \bmod 4$. Therefore, in this case, the j-invariant 1728 cannot correspond to an elliptic curve in either set $\mathcal{E}_i$.*

Remark 5.3. *By Lemma 3.5 we have $\Delta = t_i^2 - 4q_i$, from which we have*
$$q_i = \frac{t_i^2 - \Delta}{4} = \mathrm{Norm}_{K/\mathbb{Q}} \left(\frac{t_i + \sqrt{\Delta}}{2} \right).$$
It shows that q_i is the norm from K down to $\mathbb{Q}$, of the integral element
$$\pi_i = \frac{t_i + \sqrt{\Delta}}{2} \in \mathcal{O}_K.$$
Furthermore, by Remark 3.2, we obtain the relation
$$\pi_i = 1 - \overline{\pi_j}, \qquad i \neq j. \tag{1}$$

Remark 5.4. *Since Δ is not a square, the polynomial $f_i(x) = x^2 - t_i x + q_i \in \mathbb{Z}[x]$ is irreducible for $i \in \{1, 2\}$, and it is the minimal polynomial of the element $\pi_i \in \mathcal{O}_K$. In particular, $\mathbb{Z}[\pi_i]$ are both suborders of $\mathcal{O}_K$.*

Remark 5.5. *The discriminant δ_i of each order $\mathbb{Z}[\pi_i]$ can be easily computed as*

$$\delta_i = \left(\det \begin{pmatrix} 1 & \pi_i \\ 1 & \bar{\pi}_i \end{pmatrix} \right)^2 = \Delta = f^2 D.$$

Since $\pi_1 - \pi_2 = 1 - t_2$ by Remark 3.2, we also have $\mathbb{Z}[\pi_1] = \mathcal{O}_\Delta = \mathbb{Z}[\pi_2]$.

Proposition 5.6. *Let (q_1, q_2) be an odd Hasse pair. Then at least one of the base primes p_i splits completely in K.*

Proof. We equivalently show that in $\mathcal{O}_K$: (a) the p_i's cannot be both inert, and (b) if p_i ramifies, then p_j splits for $j \neq i$.

Case (a): The fact that $\mathrm{Norm}_{K/\mathbb{Q}}(\pi_i) = q_i = p_i^{a_i}$ implies that p_i is the unique prime of $\mathcal{O}_K$ that divides π_i, since $\mathcal{O}_K$ is Dedekind and we have unique factorization of ideals. Thus, for both $i \in \{1, 2\}$ there are positive integer $b_i \in \mathbb{Z}_{>0}$ such that

$$(\pi_i) = (p_i^{b_i}).$$

If both primes p_i were inert in K, by taking norms in the above equation, we would have $p_i^{a_i} = q_i = \mathrm{Norm}_{K/\mathbb{Q}}(\pi_i) = p_i^{2b_i}$. This in turn gives us that $a_i = 2b_i$ should be both even. Since $q_1 \neq q_2$, it would imply that

$$|\sqrt{q_1} - \sqrt{q_2}| = |p_1^{b_1} - p_2^{b_2}| > 1,$$

contradicting the fact that (q_1, q_2) is Hasse.

Case (b): Assume without loss of generality that p_1 ramifies in K. From Case (a) we know that only one of the exponents a_i can be even.

(i) Let us first assume that a_1 is odd. Since p_1 ramifies in $\mathcal{O}_K$, this implies that p_1 should divide the fundamental discriminant D of K, and therefore the power of p_1 dividing Δ must be odd. We recall that in the case of odd Hasse pairs, the fundamental discriminant is not divisible by 4 and is therefore squarefree. From the following relation

$$t_1^2 - 4q_1 = \Delta = f^2 D,$$

it follows that $p_1 | t_1$. Therefore, there exist $k_1 \in \mathbb{Z}$ and $b_1 \in \mathbb{Z}_{>0}$ such that $t_1 = k_1 p_1^{b_1}$, with $\gcd(k_1, p_1) = 1$. By considering the parity of the exponents of p_i in the above equation, we have that $2b_1 > a_1$. However, since $\Delta < 0$ and p_1 is odd, this case can only happen when $p_1 = 3$ and $|t_1| = 3^{\frac{a_1+1}{2}}$. This is case (d) of Theorem 2.1, which implies that $\mathcal{E}_1$ is supersingular. Proposition 4.2 now implies that $\gcd(\Delta, p_2) = 1$, from which we conclude that $\Delta = t_2^2 - 4q_2$ is a non-zero quadratic residue modulo p_2, and so is D since $D \equiv (\frac{t_2}{f})^2 \bmod p_2$. Therefore p_2 must split in K by [10, Proposition 5.16].

(ii) Assume now that a_1 is even, so a_2 is odd. Then, by Case (a) p_2 cannot be inert. From Case (b-i) above, we see that p_2 cannot ramify either, because this would imply that p_1 splits, contradicting our assumption that p_1 ramifies. Hence, p_2 must split in K. $\square$

Remark 5.7. *We note that if $\mathcal{E}_i$ is ordinary, then p_i splits because $\Delta \equiv t_i^2 \bmod p_i$. The opposite, however, might not hold, since p_i may split and divide the conductor f of Δ. In particular, Proposition 5.6 alone does not guarantee the existence of an ordinary elliptic curve in $\mathcal{E}_1 \cup \mathcal{E}_2$.*

In the case of odd Hasse pairs (p_1, p_2) with p_1, p_2 pure primes, one can conclude that both of them split completely in K unless $(p_1, p_2) = ((3, 7))$ (Example 5.8). However, this does not have to be true for prime powers with exponent > 1 (Example 5.9). Thus, the splitting of one p_i given by Proposition 5.6 is the best one can guarantee for Hasse pairs in general.

Example 5.8. *Let us consider the Hasse pair* $(3, 7)$ *as in Example 3.13, whose discriminant is* $\Delta = -3$. *By Remarks 3.12 and 5.7, this is the unique odd Hasse pair consisting of pure primes that are not both guaranteed to split completely. In fact,* $(3) = (\sqrt{-3})^2 \subset \mathcal{O}_K$ *is ramified, while* (7) *splits because* $\mathcal{E}_2$ *is ordinary (Remark 5.7).*

Example 5.9. *Since* $\sqrt{307} = 17.521\ldots$, *then* $(17^2, 307)$ *is an odd Hasse pair, whose discriminant is* $\Delta = -3 \cdot 17^2$. *As* $\mathcal{E}_2$ *is ordinary by Lemma 3.10, then* (307) *splits completely in* K *(Remark 5.7). On the other hand,* (17) *is prime (inert) in* K.

For the remainder of this section, we study under which conditions $\mathcal{E}_1 \cup \mathcal{E}_2$ may be empty.

Definition 5.10. *Let* $\mathcal{O}$ *be an order with fraction field* K. *We say that an ideal* $\mathfrak{a} \subset \mathcal{O}$ *is* proper *whenever* $\mathcal{O} = \{b \in K \mid b\mathfrak{a} = \mathfrak{a}\}$. *We recall that principal ideals are always proper [10, p. 135]. A proper* $\mathcal{O}$-*ideal is called* primitive *if it is not of the form* $d\mathfrak{a}$ *for some proper ideal* $\mathfrak{a}$ *and* $d \in \mathbb{Z}_{>0}$. *We will call an element* $\lambda \in \mathcal{O}$ *primitive if* (λ) *is a primitive ideal.*

Proposition 5.11. *Let* (q_1, q_2) *be an odd Hasse pair with corresponding traces* $t_i = k_i p_i^{b_i}$, *where* $b_i \in \mathbb{N}$ *and* $\gcd(k_i, p_i) = 1$. *Then one of the sets* $\mathcal{E}_i$ *is ordinary, except possibly when* $b_i \geq 1$, $a_i > 2b_i$ *and* $p_i^{2b_i} || \Delta$ *for both* $i \in \{1, 2\}$.

Proof. By Proposition 4.2 it is sufficient to show that if the above conditions are not satisfied, then $\mathcal{E}_1 \cup \mathcal{E}_2$ is non-empty. We show the result in steps.

Step 1: If either one of the π_i's is primitive, then $\mathcal{E}_i$ is non-empty:

(i): If $\gcd(t_i, \Delta) = 1$, then $\mathcal{E}_i$ is ordinary by Lemma 3.10.

(ii): If $\gcd(t_i, \Delta) > 1$, since π_i is primitive then in particular p_i cannot divide the conductor. This implies that p_i must divide D and hence ramifies. From Case(b-i) of Proposition 5.6, this can only happen when $p_i = 3$ and $|t_i| = 3^{\frac{a_i+1}{2}}$, which implies that $\mathcal{E}_i$ is supersingular.

Step 2: If $2b_i \geq a_i$, then $\mathcal{E}_1 \cup \mathcal{E}_2$ is non-empty:

We rewrite the norm equation

$$t_i^2 - 4q_i = p_i^{a_i}(k_i^2 p_i^{2b_i-a_i} - 4) = \Delta < 0 \implies k_i^2 p_i^{2b_i-a_i} < 4.$$

Then we must have $k_i = \pm 1$, and either

(i) $2b_i > a_i$, in which case we should have $p_i = 3$ and $\mathcal{E}_i$ is supersingular by case (d) of Theorem 2.1, or

(ii) $2b_i = a_i$, which implies that $2b_j > a_j$ and this is case (i) right above.

Step 3: Given Steps 1 and 2, $\mathcal{E}_1 \cup \mathcal{E}_2$ may be empty only if neither π_i is primitive and $2b_i < a_i$ for both $i \in \{1, 2\}$. Given the norm equation, this again implies that $p_i^{2b_i} || \Delta$ for both $i \in \{1, 2\}$. $\square$

Corollary 5.12. *If* $a_i \leq 2$ *for some* $i \in \{1, 2\}$, *then at least one of the sets* $\mathcal{E}_i$ *is ordinary.*

Proof. If for some $i \in \{1, 2\}$ we have $a_i \leq 2$, then we cannot have $a_i > 2b_i$ and $b_i \geq 1$, hence we are not in the exceptional case of Proposition 5.11. $\square$

A necessary condition for an odd Hasse pair to satisfy the exceptional conditions of Proposition 5.11 is having positive integers $a_i > 2b_i$ and odd integer primes p_i such that

$$\begin{cases} p_1^{a_1} \equiv 1 \bmod p_2^{b_2}, \\ p_2^{a_2} \equiv 1 \bmod p_1^{b_1}, \\ \left| \sqrt{p_1^{a_1}} - \sqrt{p_2^{a_2}} \right| \leq 1. \end{cases}$$

Even for $b_i = 1$, we have found no evidence of such values for moderately small prime powers ($p_i \leq 10^5$ and $a_i \leq 10^3$). Moreover, large prime powers are expected to be asymptotically "very far apart" [26, 27], therefore finding large solutions to the above inequality seems hard.

6. THE ISOGENY GRAPHS OF ORDINARY HASSE PAIRS

6.1. **The graph vertices: Sets of j-invariants.** In this section, we consider the case where both sets $\mathcal{E}_i$ are ordinary and we will refer to the pair (q_1, q_2) as an *ordinary Hasse pair*. In such cases, $\gcd(\Delta, q_1 q_2) = 1$ and Δ is odd, therefore the fundamental discriminant D is squarefree.

By Lemma 4.4 there are only two non-odd ordinary Hasse pairs, up to permutation, and it may be directly verified that their isogeny graphs (as will be defined in Section 6.2) are isomorphic (see Examples 7.2 and 7.3). Therefore, we can restrict to odd ordinary Hasse pairs and use our definitions and results from Section 5.

We recall from Remark 5.5 that the order $\mathbb{Z}[\pi_1] = \mathcal{O}_\Delta = \mathbb{Z}[\pi_2]$ is of discriminant $\Delta = f^2 D$. For any positive divisor g of f, there corresponds an order $\mathcal{O}_{g^2 D}$, with discriminant $g^2 D | \Delta$ and ideal class group $\mathrm{Cl}(\mathcal{O}_{g^2 D})$ [10, Lemma 7.2]. The cardinality $h_{g^2 D} = |\mathrm{Cl}(\mathcal{O}_{g^2 D})|$ of the ideal class group is known as the class number of $\mathcal{O}_{g^2 D}$. We denote by $H_{g^2 D}(x)$ the Hilbert class polynomial of $\mathcal{O}_{g^2 D}$ and by $L_{g^2 D}$ the splitting field of $H_{g^2 D}(x)$, also known as the ring class field of $\mathcal{O}_{g^2 D}$. Given any set of representatives $\{\mathfrak{a}_s\}_{1 \leq s \leq h_{g^2 D}}$ for $\mathrm{Cl}(\mathcal{O}_{g^2 D})$, the Hilbert class polynomial $H_{g^2 D}(x)$ is given by

$$H_{g^2 D}(x) = \prod_{1 \leq s \leq h_{g^2 D}} (x - j(\mathfrak{a}_s)) \in \mathbb{Z}[x].$$

We also have a group isomorphism $\mathrm{Cl}(\mathcal{O}_{g^2 D}) \simeq \mathrm{Gal}(L_{g^2 D}/K)$, which can be explicitly described as follows [19, Theorem 5, Chapt. 10, §3]:

$$\mathfrak{b} \mapsto \sigma_\mathfrak{b}, \quad \text{where} \quad \sigma_\mathfrak{b} j(\mathfrak{a}) = j(\mathfrak{b}^{-1} \mathfrak{a}).$$

In particular, the ideal class group $\mathrm{Cl}(\mathcal{O}_{g^2 D})$ acts on the set $\{j(\mathfrak{a}_s)\}_{1 \leq s \leq h_{g^2 D}}$ freely and transitively, and therefore $L_{g^2 D} = K(j(\mathfrak{a}))$ for any $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O}_{g^2 D})$.

Lemma 6.1. *Let (q_1, q_2) be an ordinary Hasse pair. The ideals $(\pi_i) \subset \mathcal{O}_K$ are proper, primitive, and $(\pi_i) = \mathfrak{p}_i^{a_i}$, where the $\mathfrak{p}_i$'s are prime ideals such that $\mathfrak{p}_i \bar{\mathfrak{p}}_i = (p_i)$ and $\mathfrak{p}_i \neq \bar{\mathfrak{p}}_i$.*

Proof. Since we are in the ordinary case we must have that $\gcd(t_i, \Delta) = 1$, which implies that $p_i \nmid t_i$ and $p_i \nmid f$ for both $i \in \{1, 2\}$. As a consequence [35, Lemma, §4, p. 537] both primes p_i must split in K as $p_i = \mathfrak{p}_i \bar{\mathfrak{p}}_i$, $\mathfrak{p}_i \neq \bar{\mathfrak{p}}_i$. Let us consider the norm equation

$$(q_i) = (\pi_i)(\bar{\pi}_i) = \mathfrak{p}_i^{a_i} \bar{\mathfrak{p}}_i^{a_i}.$$

Since the norms of $\mathfrak{p}_i^{a_i}$ and (π_i) are prime to the conductor, these ideals are therefore primitive and they belong to the group of ideals with unique factorization in the order $\mathcal{O}_\Delta \subseteq \mathcal{O}_K$.

We conclude that $(\pi_i) = \mathfrak{p}_i^{m_i}\overline{\mathfrak{p}}_i^{n_i}$, for some $m_i, n_i \in \mathbb{N}$ such that $m_i + n_i = a_i$. Assume by way of contradiction that both m_i, n_i are not zero. Then $p_i | \pi_i$ and therefore $p_i | t_i = \pi_i + \overline{\pi}_i$, contradiction. Therefore we have that either $m_i = 0$ or $n_i = 0$, so up to conjugation we have $(\pi_i) = \mathfrak{p}_i^{a_i}$ in $\mathcal{O}_\Delta \subseteq \mathcal{O}_K$. $\qquad\square$

Lemma 6.2. *Let (q_1, q_2) be an ordinary Hasse pair. For every $g \in \mathbb{Z}_{>0}$ with $g | f$, $H_{g^2 D}$ splits completely with distinct roots in both $\mathbb{F}_{q_i}[x]$. In particular, H_Δ splits completely with distinct roots in both $\mathbb{F}_{q_i}[x]$.*

Proof. Let us fix primes $\mathfrak{B}_i$ of $\mathcal{O}_L$ above $\mathfrak{p}_i$. Since our primes p_i neither ramify nor divide the conductor, then by [24, Proposition I.8.3], the Hilbert class polynomial H_Δ splits completely with distinct roots in both finite fields $\mathbb{F}_{p_i^{\iota_i}}$, where ι_i is called the inertia degree and it is the degree of the residue field extension

$$\iota_i = [\mathcal{O}_{L_\Delta}/\mathfrak{B}_i : \mathcal{O}_\Delta/\mathfrak{p}_i]. \tag{2}$$

Since the inertia degree is the smallest power to which the base ideal, $\mathfrak{p}_i$ in this case, becomes principal in $\mathrm{Cl}(\mathcal{O}_\Delta)$, and since $\mathfrak{p}_i^{a_i} = (\pi_i)$ by Lemma 6.1, then $\iota_i | a_i$. From the fact that $h_{g^2 D} | h_\Delta$, we have that the primes $\mathfrak{p}_i \mathcal{O}_{g^2 D}$ must also become principal when raised to a_i, for both $i \in \{1, 2\}$. Hence, by the same [24, Proposition I.8.3], $H_{g^2 D}$ must also split completely with distinct roots over both $\mathbb{F}_{q_i}[x]$. $\qquad\square$

For each $g | f$, we denote by $J_{g^2 D}$ the set of complex roots of the corresponding Hilbert Class Polynomial $H_{g^2 D}$. We note that two different $H_{g^2 D}$ cannot have common roots, and we denote by J the (disjoint) union of all these sets. We similarly denote by $J_{(g^2 D)_i}$ and J_i the sets of roots of the same polynomials in $\mathbb{F}_{q_i}$.

Remark 6.3. *Since $H_{g^2 D}$ splits completely by Lemma 6.2, the cardinality of each $J_{g^2 D}$ is $h_{g^2 D}$, i.e.*

$$|J_{g^2 D}| = |J_{(g^2 D)_1}| = |J_{(g^2 D)_2}|.$$

Therefore, we also have

$$|J| = |J_1| = |J_2|.$$

We also remark that, given Lemma 6.2, the sets $J_{(g^2 D)_i}$ are already defined in $\mathbb{F}_{p_i^{\iota_i}} \hookrightarrow \mathbb{F}_{q_i}$.

Since we are in the ordinary case, by Remark 3.9 each set $\mathcal{E}_i$ can be identified with the set of j-invariants of their elliptic curves. We note that this cannot be done in the supersingular case (Example 7.1). Remark 6.3 now implies that we can identify the sets $\mathcal{E}_i$ with J_i.

Lemma 6.4. *Let $j^{(0)} \in L$ be a root of H_Δ and r be a fixed square root of Δ. Let also $D_0 = \mathrm{Disc}(H_\Delta) \in \mathbb{Z}$. For every $j \in J$, there exists $h_j(x, y) \in \mathbb{Z}[x, y]$ such that*

$$j = \frac{h_j(j^{(0)}, r)}{2 D_0}.$$

Moreover, if p is an odd prime such that H_Δ does not have repeated roots over $\overline{\mathbb{F}}_p$, then $\gcd(2 D_0, p) = 1$.

Proof. For every order $\mathcal{O}_\Delta \subseteq \mathcal{O} \subseteq \mathcal{O}_K$ and every $j \in J$, we have $j \in L_{g^2 D} \subseteq L = K(j^{(0)})$ [19, Theorem 10.6] and $H_\mathcal{O}(j) = 0$. Since $H_\mathcal{O}$ is a monic integral polynomial, then $j \in \mathcal{O}_L$. By classical properties of simple separable extensions [24, Lemma I.2.9], we have

$$\mathcal{O}_L \subseteq D_0^{-1} \mathcal{O}_K[j^{(0)}] \subseteq (2 D_0)^{-1} \mathbb{Z}[j^{(0)}, r].$$

Thus, every $j \in \mathcal{O}_L$ can be written as $\frac{h_j(j^{(0)}, r)}{2D_0}$ for some $h_j(x) \in \mathbb{Z}[x, y]$. Moreover, since H_Δ is the minimal polynomial of $j^{(0)} \in L$ over $\mathbb{Q}$ [29, Theorem II.4.3], we have

$$D_0 = \pm \mathrm{Disc}(H_\Delta) = \pm \mathrm{Res}_x(H_\Delta(x), H'_\Delta(x)) \in \mathbb{Z}.$$

Then H_Δ has no repeated roots in $\bar{\mathbb{F}}_p$ precisely when $D_0 = \pm \mathrm{Res}_x(H_\Delta(x), H'_\Delta(x)) \in \bar{\mathbb{F}}_p^*$, i.e. when D_0 is coprime to p. $\qquad\square$

Remark 6.5. *We fix once and for all a square root r of $\Delta \in \mathbb{C}$, and an element $j^{(0)} \in J_\Delta$, which generates L_Δ over K. Now, given Remark 6.3 and Lemma 6.4, any fixed choice of a square root r_i of $\Delta \in \mathbb{F}_{p_i^{\iota_i}}$ and $j_i^{(0)} \in J_{(\Delta)_i}$, induces an explicit bijection*

$$\Pi_i : J \to J_i \subseteq \mathbb{F}_{p_i^{\iota_i}}, \qquad \frac{h_j(j^{(0)}, r)}{2D_0} \mapsto \frac{h_j(j_i^{(0)}, r_i)}{2D_0}.$$

By embedding $\mathbb{F}_{p_i^{\iota_i}}$ into $\mathbb{F}_{q_i}$, this extends to a bijection $\Pi_i : J \to J_i \subseteq \mathbb{F}_{q_i}$, which we denote in the same way. We notice that the above choices of r_i and $j_i^{(0)}$ are associated with a fixed choice of primes $\mathfrak{P}_i \subset \mathcal{O}_L$ and $\mathfrak{p}_i \subset \mathcal{O}_K$ such that $\mathfrak{P}_i | \mathfrak{p}_i | p_i$, for both $i \in \{1, 2\}$.

6.2. The Isogeny Graphs.

Definition 6.6. *Let $\mathrm{B} \subset \mathbb{N}$ be a finite set of integer primes, and $\mathcal{E}$ be a set of elliptic curves defined over a finite field $\Bbbk$, up to $\Bbbk$-isomorphism. We define the B-isogeny graph of $\mathcal{E}$, denoted by $G_\mathrm{B}(\mathcal{E})$, as the directed colored multigraph, whose vertices are the elements in $\mathcal{E}$, and the edges are cyclic $\Bbbk$-isogenies between them. The color of any edge corresponds to the degree of the isogeny, which is some prime in B.*

Remark 6.7. *When drawing isogeny graphs we use the convention that an undirected edge corresponds to one edge in each direction. We recall that $j = 1728$ can appear in an ordinary $G_\mathrm{B}(\mathcal{E})$ only in even characteristic (so it equals $j = 0$) by Remark 5.2. Since every isogeny has a dual isogeny [30, Section III.6], and $\mathrm{Aut}(E) = \{\pm\mathrm{id}\}$ for every elliptic curve E with $j(E) \neq 0, 1728$ [30, Section III.10], our graphs may be thought of as undirected, with the only possible exception of isogenies from $j = 0$.*

Lemma 6.8. *Let (q_1, q_2) be an ordinary Hasse pair. For both $i \in \{1, 2\}$, the graphs $G_{\{p_i\}}(\mathcal{E}_1)$ and $G_{\{p_i\}}(\mathcal{E}_2)$ are isomorphic and consist of h_Δ / ι_i cycles of length ι_i (as defined in (2)).*

Proof. Since the relation is symmetric, we can assume without loss of generality that $i = 2$. We can also restrict to vertices contained in $J_{(\Delta)_1}$ and $J_{(\Delta)_2}$, because all the p_2-isogenies are horizontal since (q_1, q_2) is ordinary. We compute the eigenvalues of the π_i's by examining the splitting of their minimal polynomials $f_i(x) \bmod p_2$. Given Remark 5.4, a simple computation shows that

$$f_1(x) = f_2(-x + 1).$$

We compute the eigenvalues $\{\mu_i, \nu_i\}$ of each π_i as the roots of

$$f_2(x) \equiv x(x - t_2) \bmod p_2,$$
$$f_1(x) = f_2(-x + 1) \equiv (x - 1)(x - (1 - t_2)) \bmod p_2.$$

For ordinary elliptic curves in characteristic p_2, there are only two isogenies of degree p_2: the Frobenius isogeny, which is inseparable, and its dual, called the *Verschiebung*, which is separable. The Frobenius isogeny creates cycles of length equal to the degree of the minimal

extension field where the elliptic curve is defined, which in this case is ι_2 as in (2). Therefore, the number of cycles in this case is h_Δ/ι_2.

We now look at the eigenvalues $\lambda_1 = 1$ and $\mu_1 = 1 - t_2$ of f_1. We see that $\mu_1 \not\equiv 0 \bmod p_2$ since otherwise, from the equation $q_1 = q_2 + 1 - t_2$, we would have that $p_2 | q_1$, which is not possible for odd Hasse pairs. Furthermore, $\lambda_1 \not\equiv \mu_1 \bmod p_2$, as $t_2 \equiv 0 \bmod p_2$ would lead to supersingular curves. Since we have two distinct eigenvalues, this implies that p_2 is an Elkies prime and we have h_Δ/ι_2 cycles of degree-p_2 isogenies in this case as well ([32, Theorem 7]). Thus, $G_{\{p_2\}}(\mathcal{E}_1)$ and $G_{\{p_2\}}(\mathcal{E}_2)$ have the same structure. $\square$

Theorem 6.9. *Let (q_1, q_2) be an ordinary Hasse pair and $B \subset \mathbb{N}$ be a finite set of primes. Then $G_\mathrm{B}(\mathcal{E}_1)$ is isomorphic to $G_\mathrm{B}(\mathcal{E}_2)$.*

Proof. Let $G_\mathrm{B}(\Delta)$ be the directed colored multigraph (in characteristic zero) whose vertices are the elements of J and whose edges $\phi : j_1 \to j_2$ represent isogenies of prime color $\deg \phi = \ell$ between curves with j-invariants j_1 and j_2, for any $\ell \in B$.

By adapting [29, Proposition II.4.4] to the context of Remark 6.5, for both $i \in \{1, 2\}$ we have an injection

$$\mathrm{Hom}(j_1, j_2) \to \mathrm{Hom}(\Pi_i(j_1), \Pi_i(j_2)),$$

which preserves the degree of the isogenies. Therefore, there is an isomorphic copy of $G_\mathrm{B}(\Delta)$ over both the $\mathbb{F}_{p_i^{\iota_i}}$'s. Since the isogenies, as well as the j-invariants involved, are defined over $\mathbb{F}_{p_i^{\iota_i}}$, they are also defined over $\mathbb{F}_{q_i}$, therefore the maps Π_i are isomorphic graph embeddings of $G_\mathrm{B}(\Delta)$ into the $G_\mathrm{B}(\mathcal{E}_i)$'s.

Since all the considered curves are ordinary, the structure of the isogeny graphs $G_\mathrm{B}(\Delta)$, $G_\mathrm{B}(\mathcal{E}_1)$, and $G_\mathrm{B}(\mathcal{E}_2)$ only depends on Δ. Therefore, the number and type of isogenies (horizontal or vertical) from curves with j-invariant different from 0 are the same in both characteristics (by [32, Theorem 7] and [17, Proposition 23]) for isogenies of degree $l \notin \{p_1, p_2\}$. By Lemma 6.8, the same holds for isogenies of degree p_1 and p_2.

Finally, either none or both sets $\mathcal{E}_i$ contain a curve E_i^0 with $j(E_i^0) = 0$, as this occurs if and only if the squarefree part of Δ is $D = -3$. If such curves exist, then we have

$$\mathrm{End}_{\mathbb{F}_{p_1}}(E_1^0) \simeq \mathrm{End}_{\mathbb{F}_{p_2}}(E_2^0) \simeq \mathbb{Z}\left[\frac{1 + \sqrt{-3}}{2}\right].$$

Since a j-invariant zero curve over $\mathbb{F}_{p_i^{a_i}}$ is ordinary if and only if $p_i \equiv 1 \bmod 3$, then $\sqrt{-3}$ is defined over both the $\mathbb{F}_{p_i}$'s (and consequently over the $\mathbb{F}_{q_i}$'s). Thus, in both the $G_\mathrm{B}(\mathcal{E}_i)$'s, if we have any descending l-isogenies $0 \to j \neq 0$, then there are precisely three distinct l-isogenies from 0 to j. Moreover, in this case, both the isogeny graphs have exactly $\left(\frac{\Delta}{l}\right) + 1$ isogenies of degree l from 0 to itself. $\square$

7. Examples of isogeny graphs

Example 7.1. *The discriminant of the Hasse pair $(q_1, q_2) = (4, 7)$ is $\Delta = -12$. Given $\mathbb{F}_4 = \mathbb{F}_2(\gamma) \simeq \mathbb{F}_2[x]/(x^2 + x + 1)$, one can directly verify that $\mathcal{E}_1$ contains only the following two elliptic curves*

$$0_A \; : \; y^2 + \gamma y = x^3 + 1, \qquad 0_B \; : \; y^2 + \gamma^2 y = x^3 + \gamma^2, \qquad (3)$$

which are both supersingular and their j-invariant is $0 \in \mathbb{F}_4$. On the other hand, $\mathcal{E}_2$ is ordinary and contains the curves of j-invariant 0 and $2 \in \mathbb{F}_7$. The 2-Frobenius map π_2

connects the curves 0_A and 0_B in $G_{\{2\}}(\mathcal{E}_1)$, while there are three descending and one ascending 2-isogenies in $G_{\{2\}}(\mathcal{E}_2)$. Thus, the isogeny graphs are not isomorphic as shown in Figure 1.
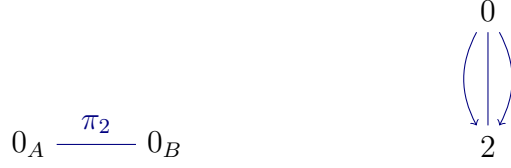

$$0_A \xrightarrow{\ \pi_2\ } 0_B$$

FIGURE 1. $\{2\}$-isogeny graphs for the Hasse pair $(4, 7)$. The curves 0_A and 0_B are defined as in (3).

Example 7.2. *The pair $(q_1, q_2) = (2, 4)$ is an ordinary Hasse pair with associated discriminant $\Delta = -7$. Given $\mathbb{F}_4 = \mathbb{F}_2(\gamma) \simeq \mathbb{F}_2[x]/(x^2 + x + 1)$, one can directly verify that $\mathcal{E}_1$ only contains the curve E_1 defined by $y^2 + xy = x^3 + 1$ over $\mathbb{F}_2$, while $\mathcal{E}_2$ only contains the curve E_2 defined by $y^2 + xy = x^3 + \gamma^2 x^2 + 1$ over $\mathbb{F}_4$, both of j-invariant 1. If π_2 is the 2-Frobenius map, one can also check that*

$$\mathrm{End}_{\mathbb{F}_2}(E_1) = \mathbb{Z}[\pi_2] = \mathrm{End}_{\mathbb{F}_4}(E_2),$$

so the isogeny graphs are isomorphic and given in Figure 2.

FIGURE 2. B-isogeny graphs $G_B(\mathcal{E}_1)$ (on the left) and of $G_B(\mathcal{E}_2)$ (on the right) for $(q_1, q_2) \in \{((2, 4)), ((4, 8))\}$ for any $2 \in B \subseteq \mathbb{N}$.

Example 7.3. *The pair $(q_1, q_2) = (4, 8)$ is the second of the two ordinary non-odd Hasse pair of Lemma 4.4, the other one being Example 7.2. The associated discriminant is again $\Delta = -7$. One can directly verify that both sets $\mathcal{E}_i$ contain only the curve defined by the model $y^2 + xy = x^3 + 1$, of j-invariant 1. Notice that in $\mathcal{E}_1$ we have the (unique) twist of E_2 from Example 7.2. Therefore the endomorphism ring for both curves is $\mathbb{Z}[\pi_2]$, and so the isogeny graphs are isomorphic and are shown again in Figure 2.*

Example 7.4. *Since $\sqrt{587} = 24.228\ldots$, then $(q_1, q_2) = (5^4, 587)$ is an odd Hasse pair, which is ordinary since its associated discriminant $\Delta = -979 = -11 \cdot 89$ is coprime with both the q_i's (Lemma 3.10). Thus, the isogeny graphs of $\mathcal{E}_1$ and $\mathcal{E}_2$ are the same by Theorem 6.9. This correspondence is portrayed for isogenies of prime degree up to 11 by Figure 3.*

Example 7.5. *Since $\sqrt{1069} - \sqrt{1021} = 0.742\ldots$, then $(q_1, q_2) = (1021, 1069)$ is an odd Hasse pair. Its associated discriminant is $\Delta = -1875 = -3 \cdot 5^4$, so both sets $\mathcal{E}_i$ are ordinary by Lemma 3.10, and their isogeny graphs are the same by Theorem 6.9. This correspondence is portrayed for isogenies of certain degrees by Figures 4 and 5.*

Example 7.6. *Since $\sqrt{22501} = 150.003\ldots$, then $(q_1, q_2) = (151^2, 22501)$ is an odd Hasse pair. Since $\Delta = -507 = -3^2 \cdot 67$, all the curves are ordinary and the isogeny graphs are isomorphic by Theorem 6.9. Those graphs are shown for isogenies of certain degrees by Figure 6. We observe that all the j-invariants of $\mathcal{E}_1$ are already defined over $\mathbb{F}_{151}$, since*

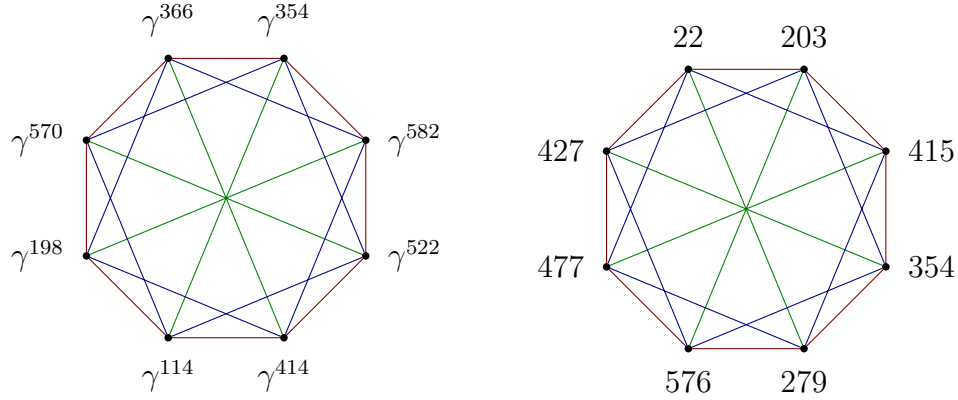FIGURE 3. $\{2,3,5,7,11\}$-isogeny graphs for the Hasse pair $(5^4, 587)$. The vertices are j-invariants over $\mathbb{F}_{5^4} = \mathbb{F}_5[\gamma] \simeq \mathbb{F}_5[x]/(x^4 + 4x^2 + 4x + 2)$ (left) and over $\mathbb{F}_{587}$ (right).
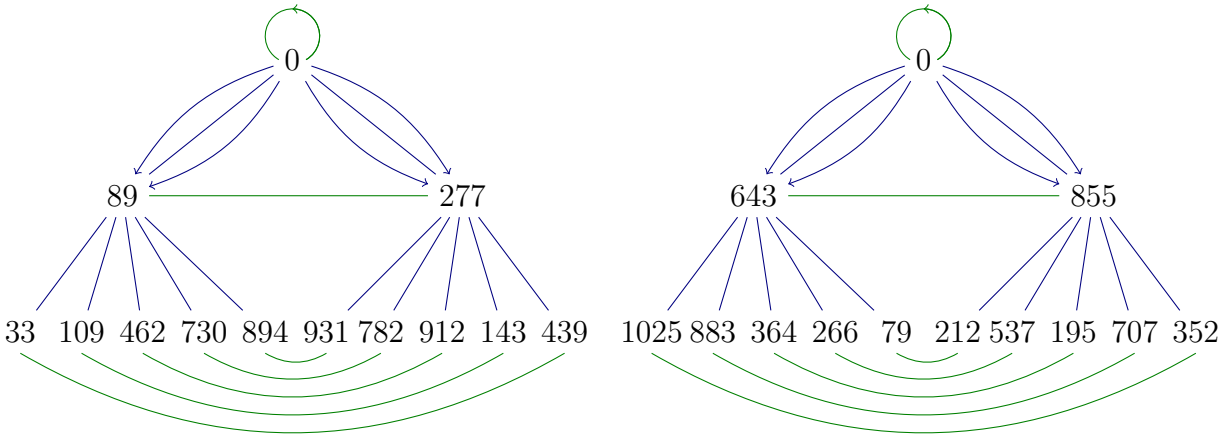

FIGURE 4. $\{3,5\}$-isogeny graph for the ordinary Hasse pair $(1021, 1069)$. The vertices are j-invariants over $\mathbb{F}_{1021}$ (left) and $\mathbb{F}_{1069}$ (right).

$\iota_1 = 1$ *(as defined in (2))*. *In fact, one can verify that the resulting isogeny graph equals the isogeny graph of (isogeny classes of) anomalous curves over $\mathbb{F}_{151}$.*

8. CONCLUSIONS

In the present paper, for a given Hasse pair (q_1, q_2) we investigated the properties of the sets $\mathcal{E}_1$ and $\mathcal{E}_2$.

When the pair is odd, the results we obtained are summarized in Table 1. In this case, we proved that $\mathcal{E}_1 \cup \mathcal{E}_2$ always contains an ordinary curve when it is non-empty, but we could not prove nor disprove whether such a union could be empty. This remains an open problem for us (Problem 1.1), and we believe that its difficulty lies in the fact that the prime powers involved should be very close, as well as meeting further modular conditions.

When the considered Hasse pair involves even entries, different cases may occur, as portrayed in Table 2. In this setting, it is possible to find only supersingular curves in $\mathcal{E}_1 \cup \mathcal{E}_2$. These cases arise precisely when we have Fermat and Mersenne primes, therefore counting
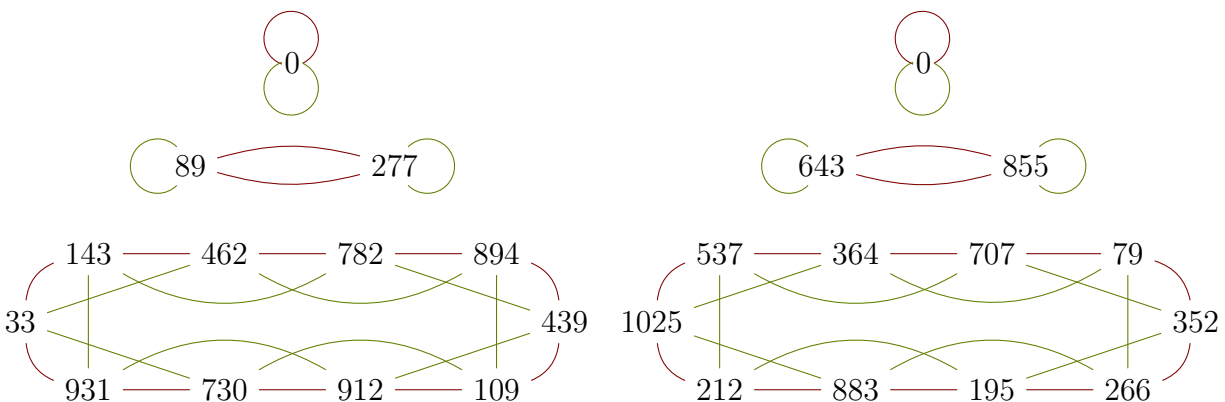
FIGURE 5. $\{7,19\}$-isogeny graph for the ordinary Hasse pair $(1021, 1069)$. The vertices are j-invariants over $\mathbb{F}_{1021}$ (left) and $\mathbb{F}_{1069}$ (right).
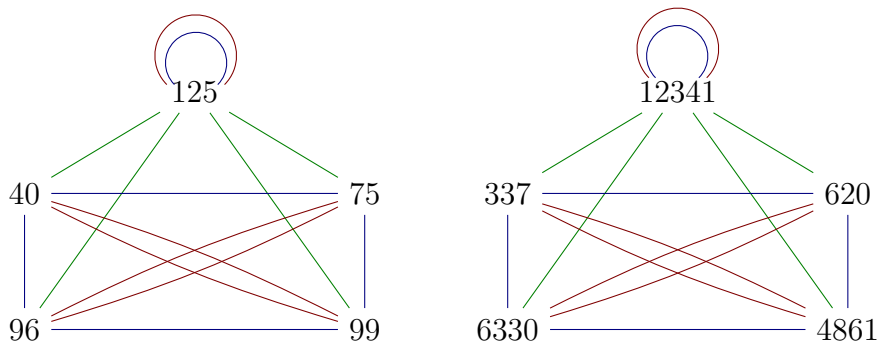

FIGURE 6. $\{3,17,19\}$-isogeny graph for the ordinary Hasse pair $(151^2, 22501)$. The vertices are j-invariants over $\mathbb{F}_{151} \hookrightarrow \mathbb{F}_{151^2}$ (left) and $\mathbb{F}_{22501}$ (right).

(q_1, q_2)		$\mathcal{E}_1$		
odd Hasse pair		ordinary	supersingular	empty
	ordinary	Same isogeny graphs Theorem 6.9	Occurs with $j = 0$ Proposition 4.3	May occur E.g. $(7^2, 43)$
$\mathcal{E}_2$	supersingular		Never occurs Proposition 4.2	
		Symmetric		
	empty	see (q_2, q_1)		Open, Problem 1.1

TABLE 1. Possible configuration arising from odd Hasse pairs.

such cases is equivalent to the well-known open problem of deciding the finiteness of these families of primes (Remark 4.7). Furthermore, the set $\mathcal{E}_i$ defined in even characteristic may be empty only if the other one (defined in odd characteristic) is also empty, but we have found only one instance of such a case. Again, the empty cases look special, and establishing a complete classification of them seems challenging.

Furthermore, in the last section we observed that, regardless of the characteristic, when $\mathcal{E}_1$ and $\mathcal{E}_2$ are both ordinary, we have a perfect correspondence between their isogeny graphs. This relation is effective only on paper at the moment, as we lack an efficient way of passing

$(2^{a_1}, q_2)$		$\mathcal{E}_1$		
Hasse pair		ordinary	supersingular	empty
	ordinary	q_2 even, classified Lemma 4.4	May occur Example 7.1	May occur E.g. $(2^4, 11)$
$\mathcal{E}_2$	supersingular	Never occurs Lemma 4.4	Classified Theorem 4.6	May occur E.g. $(2^3, 7)$
	empty		Never occurs Theorem 4.6	May occur E.g. $(2^8, 3^5)$

TABLE 2. Possible configuration arising from non-odd Hasse pairs.

from one isogeny graph to the other. Performing such correspondence efficiently, i.e. without passing through the construction of huge Hilbert class polynomials in characteristic zero, is regarded as an ambitious task, which could lead to interesting cryptographic applications.

Finally, similarly to how aliquot cycles extend the idea of amicable primes [31], one may aim at extending the ideas of the current paper by considering the tuples $(p_1^{a_1}, \ldots, p_r^{a_r})$ of prime powers and elliptic curves $E_1, \ldots, E_r$, such that for every $1 \le i \le r$, the curve E_i is defined over $\mathbb{F}_{q_i}$ and

$$\forall\, 1 \le i \le r - 1 \ : \ |E_i| = q_{i+1}, \quad |E_r| = q_1.$$

When ordinary, all these curves should have the same isogeny graphs.

ACKNOWLEDGEMENTS

APPENDIX A. HASSE PAIRS AND ANDRICA'S CONJECTURE
BY PIETER MOREE AND EFTHYMIOS SOFOS

Recall that a pair of distinct prime powers (q_1, q_2) is called a *Hasse pair* if

$$|\, \sqrt{q_1} - \sqrt{q_2}\, | \le 1. \tag{4}$$

If both q_1 and q_2 are odd, then the pair is called an *odd Hasse pair*. Using Lemma 4.5 it is easy to see that if $\sqrt{q_1} - \sqrt{q_2} = 1$, then necessarily $q_1 = 81$ and $q_2 = 64$, thus replacing ≤ 1 by < 1 is almost equivalent.

It is natural to ask if there are many Hasse pairs. In this direction we contribute the following result.

Theorem A.1. *Fix any $\epsilon > 0$. There exists a constant $c(\epsilon)$ such that for every real number $x \ge 2$ and almost all primes $p < x$, with at most $c(\epsilon)\, x^{3/5+\epsilon}$ exceptions, there are at least $\frac{1}{2}\sqrt{p}\,(\log p)^{-1}$ Hasse pairs (p, ℓ) with ℓ a prime.*

We will apply some ideas from analytic number theory to this question. Since the number of primes up to x grows asymptotically as $x/\log x$ and the number of prime powers p^m with $m \geq 2$ only as $\sqrt{x}$, which is $\leq c(\epsilon)\, x^{3/5+\epsilon}$ for every x sufficiently large, we see that Theorem A.1 implies the following corollary.

Corollary A.2. *Theorem A.1 also holds true if instead of primes we consider prime powers.*

Thus typically a large prime (power) occurs as a member of a *large number* of Hasse pairs. However, we cannot exclude the existence of a prime power that *never* occurs as a member of a Hasse pair.

Conjecture 1. *Every prime power is a member of some Hasse pair.*
Every odd prime power is a member of some odd Hasse pair.

In Section A.2 we show that this conjecture is intimately connected with Andrica's conjecture. Research on that conjecture then shows that Conjecture 1 is certainly true for all prime powers $< 10^{19}$. Let $p_1 = 2, p_2 = 3, \dots$ be the sequence of consecutive primes.

Proposition A.3. *If Andrica's conjecture that (p_j, p_{j+1}) is always a Hasse pair is true, then so is Conjecture 1.*

Proof. If q is a prime power, we let p_j be the largest prime $\leq q$. Then (q, p_{j+1}) is a Hasse pair by Andrica's conjecture. If q is odd, then (q, p_{j+1}) is an odd Hasse pair. $\square$

A.1. **Proof of Theorem A.1.** Theorem A.1 is in essence a corollary of the following deep result due to Heath-Brown [13].

Theorem A.4 (Heath-Brown [13]). *For any fixed $\epsilon > 0$ the measure of the set of $y \in [0, x]$ such that*

$$\max_{0 \leq h \leq \sqrt{y}} \left| \pi(y+h) - \pi(y) - \int_y^{y+h} \frac{\mathrm{d}t}{\log t} \right| \geq \frac{\sqrt{y}}{(\log y)(\log \log y)}$$

is $O_\epsilon(x^{3/5+\epsilon})$.

Proof of Theorem A.1: Let B_x be the set of primes $p \in [2, x]$ such that the interval $(p, p+\sqrt{p})$ contains $\leq \sqrt{p}/(2\log p)$ primes. Our plan is to show that for any $p \in B_x \cap [2, x-1]$ the interval $(p, p+1)$ contributes towards the measure in Theorem A.4, from which we can directly deduce that the number of elements in B_x is bounded above by $c(\epsilon)\, x^{3/5+\epsilon}$.

For any $p \in B_x$ and $y \in (p, p+1)$ we have that the number of primes in the interval $(y, y+\sqrt{p})$ is at most 2 plus the number of primes in the interval $(p, p+\sqrt{p})$, which by assumption is $\leq 2 + \sqrt{p}/(2\log p)$. Now for all sufficiently large p by trivial calculus this is $\leq \sqrt{p}/(\log 2p) - \sqrt{p+1}/(\log(p+1)\log\log(p+1))$ and by the monotonicity of the log function this is

$$\leq \int_y^{y+\sqrt{p}} \frac{\mathrm{d}t}{\log t} - \frac{\sqrt{p+1}}{\log(p+1)\log\log(p+1)},$$

but since $y < p+1$, we finally conclude that

$$\pi(y+h) - \pi(y) \leq \int_y^{y+\sqrt{p}} \frac{\mathrm{d}t}{\log t} - \frac{\sqrt{y}}{\log y \log\log y}.$$

Now taking $h = \sqrt{p}$ in Theorem A.4, we note that $h \leq \sqrt{y}$ and hence we have shown that if $p \in B_x$, then every y in the interval $(p, p+1)$ satisfies the inequality in Theorem A.4, showing that the number of elements in B_x is bounded above by $c(\epsilon)\, x^{3/5+\epsilon}$. $\square$

A.2. **Andrica's conjecture.** Let $d_n := p_{n+1} - p_n$ be the nth prime gap. Over the centuries many conjectures involving d_n have been made. Here we are interested in a conjecture made in 1986 by Dorin Andrica [1].

Conjecture 2 (Andrica [1]). *The inequality*

$$\sqrt{p_{n+1}} - \sqrt{p_n} < 1 \tag{5}$$

holds for all n.

A lot of numerical work on large gaps has been done. This can be used to infer that Andrica's conjecture holds for $p_n \leq 2 \cdot 2^{63} \approx 1.8 \cdot 10^{19}$; see Visser [33].

An equivalent formulation of Andrica's conjecture is that

$$d_n < 2\sqrt{p_n} + 1 \tag{6}$$

holds for all n. It seems to be far out of reach, as under RH the best result is due to Cramér [11] who showed in already 1920 that $d_n = O(\sqrt{p_n} \log p_n)$. More explicitly, Carneiro et al. [8] showed under RH that $d_n \leq \frac{22}{25}\sqrt{p_n} \log p_n$ for every $p_n > 3$. Unconditionally Baker et al. [3] showed that $d_n < p_n^{0.525}$ for all n sufficiently large.

Heath-Brown used Theorem A.4 to obtain the following result on large gaps between consecutive primes, which is a culmination of an enormous amount of research done over many years.

Theorem A.5 (Heath-Brown [13]). *We have*

$$\sum_{\substack{p_n \leq x \\ p_{n+1} - p_n \geq \sqrt{p_n}}} (p_{n+1} - p_n) \ll_\epsilon x^{3/5+\epsilon}.$$

For a table of earlier (larger) exponents than $3/5$ achieved and their authors, see Moree [23].

The authors (with Kosyak and Zhang) [18] came across the quantity on the left hand side in Theorem A.5 as essentially being the number of failures up to x for a method of construction they have for producing cyclotomic polynomials $\Phi_n(x)$ having maximum coefficient h, with $h \leq x$. If a slightly stronger variant of Andrica's conjecture holds true, then they showed that *every* natural number occurs as maximum coefficient of some cyclotomic polynomial. For a more leisurely account, see Moree [23].

A.3. **Andrica's conjecture for denser sequences.** In our context a slightly weaker version of Andrica's conjecture comes up, namely:

Conjecture 3 (Andrica for prime powers). *Let $q_1, q_2, \ldots$ be the consecutive prime powers. The inequality*

$$\sqrt{q_{n+1}} - \sqrt{q_n} < 1 \tag{7}$$

holds for all n.

Since the number of primes up to x grows asymptotically as $x/\log x$ and the number of prime powers p^m with $m \geq 2$ as $\sqrt{x}$, this modified version is, unfortunately, not that much weaker. One could hope that if one replaces the sequence of prime numbers by a substantially 'fatter' sequence, one might be able to prove the analogue of Andrica's conjecture. Finally, we present an example showing that this hope is not unjustified.

A positive integer n is said to be *practical* if every positive integer $\leq n$ is a subset-sum of the positive divisors of n. Weingartner [36] showed that there is a constant $c = 1.33607\ldots$ such that the number of practical numbers $\leq x$ grows as $cx/\log x$. The analogue of Andrica's conjecture for the practical numbers is known to be true, see Wu [37].

Max-Planck-Institut für Mathematik,
Vivatsgasse 7, D-53111 Bonn, Germany.
E-mail: `moree@mpim-bonn.mpg.de`

School of Mathematics and Statistics,
University of Glasgow,
University Place, Glasgow, G12 8SQ, United Kingdom.
E-mail: `efthymios.sofos@glasgow.ac.uk`

References

1. D. Andrica, Note on a conjecture in prime number theory, *Studia Univ. Babeş-Bolyai Math. 31*, 1986, pp. 44–48.
2. D. F. Aranha, Y. El Housni, A. Guillevic, A survey of elliptic curves for proof systems, *Des. Codes Cryptogr. 91*, 2023, pp. 3333–3378.
3. R. C. Baker, G. Harman, J. Pintz, The difference between consecutive primes, II, *Proc. London Math. Soc. 83*, 2001, pp. 532–562.
4. M. Bellés-Muñoz, J. J. Urroz, J. Silva, *Revisiting Cycles of Pairing-Friendly Elliptic Curves*, In CRYPTO 2023, Springer Cham, pp. 3–37.
5. E. Ben-Sasson, A. Chiesa, E. Tromer, M. Virza, *Scalable Zero Knowledge via Cycles of Elliptic Curves*, In CRYPTO 2014, Springer Berlin Heidelberg, pp. 276–294.
6. S. Bowe, J. Grigg, D. Hopwood, *Halo: Recursive proof composition without a trusted setup*, Cryptology ePrint Archive, Paper 2019/1021.
7. J. Brown, D. Heras, K. James, R. Keaton, A. Qian, Amicable pairs and aliquot cycles for elliptic curves over number fields, *Rocky Mt. J. Math. 46*, 2016, pp. 1853–1866.
8. E. Carneiro, M. B. Milinovich, K. Soundararajan, Fourier optimization and prime gaps, *Comment. Math. Helv. 94*, 2019, pp. 533–568.
9. A. Chiesa, L. Chua, M. Weidner, On Cycles of Pairing-Friendly Elliptic Curves, *SIAM J. Appl. Algebra Geom. 3*, 2019, pp. 175–192.
10. D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, Class Field Theory and Complex Multiplication*, Wiley, 1989.
11. H. Cramér, Some theorems concerning prime numbers, *Arkiv f. Math. Astr. Fys. 15*, 1920, pp. 1–33. [Collected Works 1, 85–91, Springer, Berlin-Heidelberg, 1994.]
12. M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, *Abh. Math. Semin. Hansische Univ. 14*, 1941, pp. 197–272.
13. D. R. Heath-Brown, The differences between consecutive primes, V, *Int. Math. Res. Not. IMRN 22*, 2021, pp. 17514–17562.
14. D. Hopwood, *Pluto-eris hybrid cycle of elliptic curves*, 2021, available at `https://github.com/daira/pluto-eris`.
15. D. Hopwood, *The pasta curves for halo 2 and beyond*, 2020, available at `https://electriccoin.co/blog/the-pasta-curves-for-halo-2-and-beyond/`.
16. N. Jones, Elliptic aliquot cycles of fixed length, *Pac. J. Math. 263*, 2013, pp. 353–371.
17. D. Kohel, *Endomorphism rings of elliptic curves over finite fields*, PhD thesis, University of California, Berkeley, 1996.
18. A. Kosyak, P. Moree, E. Sofos, B. Zhang, Cyclotomic polynomials with prescribed height and prime number theory, *Mathematika 67*, 2021, pp. 214–234.

19. S. Lang, *Elliptic functions*, Springer, 1987.
20. I. Meckler, *O(1) labs fork of zexe: implementation of bn382-plain*, 2020, available at `https://github.com/o1-labs/zexe/tree/master/algebra/src/bn_382`.
21. P. Mihăilescu, *Dual Elliptic Primes and Applications to Cyclotomy Primality Proving*, ArXiv: 0709.4113.
22. P. Mihăilescu, Primary Cyclotomic Units and a Proof of Catalan's Conjecture, *J. Reine Angew. Math. 572*, 2004, pp. 167–195.
23. P. Moree, Prime gaps and cyclotomic polynomials, *Nieuw Arch. Wisk. 5/22*, 2021, pp. 219–225.
24. J. Neukirch, *Algebraic Number Theory, Translated from the German by Norbert Schappacher*, Springer-Verlag, Berlin Heidenberg New York, 1999.
25. J. Parks, An asymptotic for the average number of amicable pairs for elliptic curves, *Math. Proc. Camb. Philos. Soc. 166*, 2019, pp. 33–59.
26. S. S. Pillai, On $a^x - b^y = c$, *J. Indian Math. Soc. 2*, 1936, pp. 119–122.
27. S. S. Pillai, A correction to the paper "On $a^x - b^y = c$", *J. Indian Math. Soc. 2*, 1937, p. 215.
28. P. Ribenboim, *Catalan's Conjecture: Are 8 and 9 the only Consecutive Powers?*, Academic Press, Inc. 1994.
29. J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, 1994.
30. J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd edition, Springer, 2008.
31. J. H. Silverman, K. E. Stange, Amicable Pairs and Aliquot Cycles for Elliptic Curves, *Exp. Math. 20*, 2011, pp. 329–357.
32. A. V. Sutherland, *Isogeny volcanoes*, In ANTS X. Open Book Series 1, 2012, pp. 507–530.
33. M. Visser, Strong version of Andrica's conjecture, *Int. Math. Forum 14*, 2019, pp. 181–188.
34. S. S. Wagstaff, Divisors of Mersenne numbers, *Math. Comp. 40*, 1983, pp. 385–397.
35. W. Waterhouse, Abelian varieties over finite fields, *Ann. Sci. Ècole Norm. Sup. 2*, 1969, pp. 521–560.
36. A. Weingartner, The constant factor in the asymptotic for practical numbers, *Int. J. Number Theory 16*, 2020, pp. 629–638.
37. X.-H. Wu, Special forms and the distribution of practical numbers, *Acta Math. Hungar. 160*, 2020, pp. 405–411.

Max-Planck-Institut für Mathematik,
Vivatsgasse 7, D-53111 Bonn, Germany.
Email address: agathocleous@mpim-bonn.mpg.de

CISPA Helmholtz Center for Information Security,
Stuhlsatzenhaus 5, 66123 Saarbrücken, Germany.
Email address: joux@cispa.de

KU Leuven,
Celestijnenlaan 200A - box 2402, 3001 Leuven, Belgium.
Email address: daniele.taufer@kuleuven.be