Eurocrypt'23 reviews and differences with Crypto'23 submission

Revisiting cycles of pairing-friendly elliptic curves

This supplementary material contains (1) the original Eurocrypt'23 reviews, (2) how we addressed the suggestions of the reviewers, and (3) a version of the manuscript highlighting the changes from the Eurocrypt'23 to the Crypto'23 submissions. Note that, in particular, some notation was changed, and some theorems and lemmas were renumbered. As a result, some of the reviewers' comments may not match the current version of the paper.

Review #94A

Paper summary. This paper revisits cycles of pairing-friendly elliptic curves. Such cycles are very useful in the context of verifiable computing. The optimal case are 2-cycles for which the base field prime of one curve is equal to the group order of the other and vice versa. Finding cycles (other than ones from MNT4-MNT6 curves) is very hard and they might not even exist. With the goal of better understanding and possibly discovering new cycles, the paper studies their properties and shows new results that rule out some known parameterized curve families. It is mainly a continuation of previous work by Chiesa, Chua and Weidner and refines some of their results.

Overall merit. Weak accept (I have more arguments in favor of accept).

Reviewer expertise. Expert (I've worked on this topic domain and I'm familiar with the literature).

Confidence level. High (Carefully read and understood the main submission and checked relevant parts of the supplementary material).

Questions/clarifications for the authors.

1. Clarification in Lemma 5.5: This Lemma remains unclear to me. Could you please check that the statement is correct? The inequalities bounding the cardinality of $C_s(X)$ involve the value K, but $C_s(X)$ is independent of K, is it not? The lower case k should be an upper case K in $C_{s,K}(X)$, right?

   Unfortunately, I was not able to convince myself that the proof is correct. Please make it more clear. The induction is not easy to understand although it should be. I think one can very easily prove similarly to what you do that for two consecutive primes we have $|\sqrt{(q_{i+1})} - \sqrt{q_i}| < 1$ and more general $|\sqrt{(q_{i+\ell})} - \sqrt{q_i}| < \ell$. Then it follows that the q_i all lie in I_i because they form a circle. It took way too long for me to understand this given your proof. Please see below for more comments on that proof.

2. Clarification in Lemma 4.4: The statement is not precise. I think that the condition that all $r(x)$ have the same sign needs to be covered by the existence of A and B. I suggest to state the following: "...

there exist A, B such that for all $x < A$, $\text{sign}(r(x))$ is constant, such that for all $x > B$ $\text{sign}(r(x))$ is constant, and such that for all x not in $[A, B]$, either $r_x = ...$". Is this correct?

Technical details. This paper mainly continues the work started by Chiesa, Chua and Weidner with the goal of finding new cycles of pairing-friendly curves, or maybe, to better understand why there are so few of them.

The main result about 2-cycles shows that if a curve from a polynomial family is part of the cycle, then the other curve is from a family for which all divisibility conditions hold for the polynomials or it is one of a finite set of curves. This result allows to exhaust all possibilities for the known families and allows to rule out certain options. Some of these results were not known before, for example that Freeman and BN curves cannot occur in 2-cycles with other curves of embedding degree ≤ 20.

The authors also prove some bounds on the trace of curves in 2-cycles, which leads to the new insight that for polynomial families in 2-cycles with embedding degree 8 or 12, the trace of Frobenius lies at the outer edge of the Hasse interval. This can help in searches because the trace polynomial must have degree $\deg(p)/2$.

Towards the end of the introductory Section 2 the authors present a speedup to an algorithm (suggested by Freeman) that searches prime order pairing-friendly curves, but the authors weren't able to find any more families with that. It is likely that Freeman, Scott and Teske already ran such experiments on a very large scale and didn't find any new families. The result here is not surprising, but recording the algorithm variant is valuable.

Some specific remarks:

- Typo in Remark 4.6: Clearly, the Freeman $p \mod q$ is not of the form where the quadratic term has coefficient $25b$. I think you mean $5b$. The argument should go through with that change. Please confirm that it works.

- Proof of Lemma 5.2: Please use the floor of $\sqrt{X/C}$ when first defining the range for k and in the sum over the π_k, etc. Also Equation (3) is wrong, it needs to be $2N/\log(N)$ on the right hand side. You use it correctly in what follows, though.

- Proof of Lemma 5.5 needs to be made more clear: p_i in the third line should be q_i. Please simplify the proof to show that all q_i are in I_i as noted above. The inequality from Lenstra's paper must be $|\ell - (q + 1)| \leq 2\sqrt{q}$. What is the cardinality of L you use to arrive at the upper bound for $C_s(X)$?

- I think that using the same letter c or C for constants that change during a proof or an argument makes it really hard to understand these proofs. Why not at least number them c_1, c_2, c_3, etc. to make it clear that the constants change?

Minor remarks:

- The term "constant-time" usually means that code is written such that its execution time is independent of any secret data. You mean constant verification time, which is something else.

- In Prop. 2.8, please don't use $\Phi_k \circ t$ for $\Phi_k(t - 1)$.

- In the proof of Lemma 3.7, I don't think one needs the convergence of the geometric series, one can show the same simply using the finite geometric sum.

- In Prop. 3.10 and Cor. 3.11, fix the condition on k to be $3 \leq k \leq 104$.
- It seems to me that stating Prop. 4.1 in a positive way is simpler: if the previous curve has embedding degree ℓ, then there exists i s.t. $q(i) = 1 \mod \ell$?
- Thm. 4.5. The statement needs to end with "embedding degree ℓ."
- Third line after proof of Thm. 4.5: "it is immediate to check whether $q|p^\ell - 1$".
- Proof of Lemma 5.4: $h^{k_i} - 1$ must be $h_i^{k_i} - 1$.
- Reference 32: The title must be "Zur Theorie der Kreisteilungsgleichung".

Editorial details. The editorial quality is decent. Some technical details are imprecise and there are quite a few typos, none of them seem to be actual errors. A few places could be written much clearer as indicated in my above remarks, but overall I could understand the paper.

Novelty and conceptual contributions. The paper extends what is known about cycles of pairing-friendly curves. Although there are no new constructions, showing where not to look is valuable too. With verifiable computing and SNARKs being at the center of many applications where performance and scalability are important, it is natural to ask whether more efficient parameters exist. While this paper might be of interest for only a smaller fraction of the Eurocrypt audience, it is interesting for everyone trying to implement and use such protocols.

Review #94B

Paper summary. This paper investigates pairing-friendly elliptic curves and 2-cycle property. The authors examine existing families of pairing-friendly elliptic curves, and demonstrate the non-existence of 2-cycle properties.

Overall merit. Weak reject (I have more arguments in favor of reject).

Reviewer expertise. Some familiarity (I have not worked on this topic domain but I am superficially familiar with the literature).

Confidence level. Low (Read as much of the main submission as possible, but got stuck in parts).

Technical details. The authors mainly focus on the 2-cycle properties of pairing-friendly elliptic curves with the motivation on applications to proof systems such as SNARKs which involves pairings. The paper provides background on pairing-friendly elliptic curves and cycles of elliptic curves. These are nice, but I believe they can be shorten and made more concise. The authors then present the analysis on 2-cycle in elliptic curves. It would be good if the authors could also explain the significance or the impact of the findings. For example, where are the mentioned families of pairing-friendly curves are used and how knowing the cycles are useful in a real application.

Editorial details. The editorial quality is reasonable but can be improved. It might be good to clearly highlight new contributions.

Novelty and conceptual contributions. The main result of this paper is to show the (non-) existence of s-cycle of elliptic curves, with the focus on pairing-friendly curves. The authors provide many propositions, theorems, lemmas, and corollaries. The proofs and the analysis of existing families of pairing-friendly curves are good to know.

Review #94C

Paper summary. This paper is about ways and dead-ends in finding cycles of pairing-friendly elliptic curves, with recursive SNARKs as main application. This paper is about a mathematical aspect of elliptic curves defined over prime fields. More precisely, it aims at finding parameters and families of elliptic curves satisfying many constraints:

- 2-cycle: $E_1/\mathbb{F}_q$ has order p, $E_2/\mathbb{F}_p$ has order q (the role of p and q are swapped),
- prime order: $\#E_1(\mathbb{F}_q) = p$, $\#E_2(\mathbb{F}_p) = q$ and p, q are prime integers,
- pairing-friendly: E_1 and E_2 are pairing-friendly, that is, they have a low embedding degree (the smallest integer w.r.t. the subgroup order p, resp. q, such that the p-torsion, resp. q-torsion is $\mathbb{F}_{q^{k_1}}$, resp. $\mathbb{F}_{p^{k_2}}$-rational, in other words, one can compute a Weil or Tate pairing efficiently.

This work is based on the paper [13].

[13] Chiesa, A., Chua, L., Weidner, M.: On cycles of pairing-friendly elliptic curves. *SIAM Journal on Applied Algebra and Geometry* 3(2), 175-192 (2019) https://epubs.siam.org/doi/epdf/10.1137/18M1173708.

It explores some of the open questions of [13]. It has an editorial quality that could be improved to help the reader understanding better the results and their consequences. The new contributions of this paper are presented pages 10-21. Sect. 3.2 presents lemmas and results on bounds that the values of cyclotomic polynomials can take. Sect. 4 has impossibility results on cycles where one of the curves has parameters of a known family of pairing-friendly curve of prime order. Section 5 has probabilities on the density of s-cycles of curves in the way Balasubramanian and Koblitz did for pairing-friendly curves. The paper has appendices and comes with SageMath code. Section 3 contains preliminary results required in Section 4. Section 4 proves that one cannot make a 2-cycle where one of the two curves is a pairing-friendly curve in a known family: Freeman curves, BN curves, MNT3 curves, and the other one is a (yet unknown) curve of embedding degree less than 20. The only case that works is the already known case of MNT4+MNT6. It seems that the same technique would work to enlarge the bound of 20 on the second embedding degree (it would require more computing time to fill-in tables of Appendix B).

Overall merit. Weak accept (I have more arguments in favor of accept).

Reviewer expertise. Expert (I've worked on this topic domain and I'm familiar with the literature).

Confidence level. High (Carefully read and understood the main submission and checked relevant parts of the supplementary material).

Questions/clarifications for the authors.

1. I have some clarifications requests about pages 8-9 and the algorithm page 8. The authors present an algorithm à la Tanaka-Nakamula [TN08] for finding polynomial parameters of pairing-friendly elliptic curves, that is, polynomials $(p(x), q(x), t(x))$ where t is the trace, q is the field characteristic, and p is the prime order. Somehow, this is related to the KSS technique. [SG18] presented in a unified setting the known BN, Freeman and MNT curves, thanks to the Aurifeuillean factorization of cyclotomic polynomials. In the submitted paper, the authors cite [23], but later there was [GP06] and [W12]. Except for $k = 8$ which was considered in [TN08] and [KSS08], it seems to me that the Aurifeuillian technique [GP06] captures all possible cases of factorization of cyclotomic polynomials $\Phi_k(t(x) - 1)$ where $\deg(t) = 2$. Could the authors comment on that? [updated] The authors answered my questions.

   [GP06] Andrew Granville and Peter Pleasants. Aurifeuillian factorization. Math. Comp., 75(253):497-508, 2006. https://www.ams.org/journals/mcom/2006-75-253/S0025-5718-05-01766-7.

   [KSS08] Kachisa, Schaefer, Scott. Constructing Brezing-Weng pairing friendly elliptic curves using elements in the cyclotomic field. https://eprint.iacr.org/2007/452.

   [SG18] Scott and Guillevic. A new family of pairing-friendly elliptic curves. WAIFI 2018. https://eprint.iacr.org/2018/193.

   [TN08] Tanaka S., Nakamula K.: Constructing pairing-friendly elliptic curves using factorization of cyclotomic polynomials. In: Galbraith S.D., Paterson K.G. (eds.) PAIRING 2008. LNCS, vol. 5209, pp. 136-145. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-85538-5_10.

   [W12] Samuel S Wagstaff, Jr. The search for Aurifeuillian-like factorizations. Journal of Integers, 12A(6):1449-1461, 2012. https://homes.cerias.purdue.edu/ ssw/cun/mine.pdf.

2. Section 5 contains number theory results. Could the authors comment on their formulas, link the results of the section to the rest of the paper, and explain what are the consequences in the possibility of finding s-cycles of pairing-friendly curves?

3. I have another request about appendix C3, function `is_integer_valued()`. Is this function testing if a polynomial with coefficients in `QQ` takes only integer values? Why is it not needed to compute the congruences of x such that $g(x)$ is in `ZZ`, e.g. $x = 1 \mod 3$ would give integer values but $x = 0, -1$ would not. For example for BLS12 curves (that are not of prime order and will never form a 2-cycle), $q(x)$ has the form $(x - 1)^2/3 * p(x) + x$, and takes integer values only at $x = 1 \mod 3$.

I agree with the authors' answers. My remark about `is_integer_valued()` is meaningless.

Technical details. About Proposition 3.9: (I checked it) `t > ((t-1)/t * q)^(1/euler_phi(k))`. If we consider the MNT parameters e.g. given by Ben Lynn code, we can check this formula on numerical data:

```
k = 4
u = ZZ(-0x72a74a7ba34d61b0)
D = ZZ(684811)
t = u+1
q = u**2+u+1
p = u**2+1
y = ZZ(0x3d6ee0031aa423)
Fq = GF(q)
a = -3
b = ZZ(0xc4eb66bd690a0b02bdbf8f38bf33148)
E = EllipticCurve([Fq(a), Fq(b)])
assert E.order() == p
assert p.is_prime()

assert q + 1 - t == p
assert t**2 - 4*q == -D*y**2

t_ = t.abs()
assert t_**euler_phi(k) * t_ > ((t_-1) * q)
assert t_  > ((t_-1)/t_ * q)**(1/euler_phi(k))
```

Editorial details. The paper could say more explicitly what are the consequences of the results in practice.

- For example what does Proposition 3.6 imply? Is it true to deduce that a polynomial family with $\deg(t)$ even (t is the trace) will never be a node in a s-cycle? (unlike MNT-4 and MNT-6 curves, that have $\deg(t) = 1$ and form a polynomial 2-cycle). Or is it more subtle? Maybe part (b) of the introduction of Section 4 is related?
- End of Sect. 3 says: "this is consistent with what is observed in known families". What are the known families the sentence refers to? As far as we know, only BN curves are known as prime-order pairing-friendly curves with $k = 12$, and none for $k = 8$, right? In the BN case, indeed, one can check that $q/4 < t^2 < 4 * q$ (taking the squares). Is that what this sentence means?
  `QQx.<x> = QQ[]; t = 6*x^2+1; q = 36*x^4+36*x^3+24*x^2+6*x+1;`
- Lemma 4.4. I agree with reviewer #A about the statements on A and B.

Minor remarks and typos:

- p. 3 Notation. "that p, q, $q_i > 3$ and are prime" → "that p, q, and $q_i > 3$ are prime"
- p.10 I would suggest writing "$\#E(\mathbb{F}_q)$ is in the Hasse interval of $\#E'(\mathbb{F}_p)$ if and only if $\#E'(\mathbb{F}_p)$ is in the Hasse interval of $\#E(\mathbb{F}_q)$", that is, writing explicitly that is it about orders over the respective ground fields.
- p. 12 According to the notations of Remark 3.2, the second curve in Proposition 3.10 and in Corollary 3.11 should be labeled E', not E.
- p. 13 Sect. 4.1 first line, "will that" → "that will". A comma is missing at the end of the second line of numbers in Corollary 4.2, after the number 70.
- Bottom of page 14 in Lemma 4.4: replacing the end comma with a full stop?

Novelty and conceptual contributions. The new results are exposed mainly in sect. 4 and 5. Section 4 presents an interesting technique to prove impossibility results on finding 2-cycles. Sect. 5 deals with the density of s-cycles of pairing-friendly curves and builds on the work of Balasubramanian and Koblitz. It would help understanding these contributions if the authors could better explain what they are doing and the implications of the results.

Final reviewer consensus

All reviewers agree that studying cycles of pairing-friendly elliptic curves is an interesting and timely topic, in particular given the strong interest to construct more efficient SNARKs by providing better parameters than those given by the inefficient MNT cycle, which currently is the only option. The results, in particular the method described in Section 4, are interesting.

We thank the authors for their detailed answers to the reviewers' questions. While we think that this is a promising paper and that negative results like yours have a place in the literature, in the end we concluded that the paper is not yet in a shape to be accepted at Eurocrypt. The number of typos and some inaccuracies have made it hard to verify the results and understand the paper fully.

We encourage the authors to improve their paper and submit their work again. Please fix typos, consider improving the exposition to better explain the results, include the references pointed out by the reviewers and adjust the section about the search algorithm accordingly. Consider better connecting Section 5 to the rest. The reviews and the authors responses should be a good guide.

Author's answers to first set of reviews

We thank the committee for their thoroughness in reviewing the paper, and for providing us with very valuable feedback. We have considered and implemented most of the smaller comments, fixing the typos and incorporating necessary clarifications.

We answer the main concerns of the reviewers below.

Review #94A

1. Lemma 5.5. Indeed, both the statement and proof of this lemma had a few inaccuracies. In particular, $C_s(X)$ is independent of K, and the factor K which appeared in both the lower and upper bound should be removed. Also, the notation $C_{s,k}$ should be $C_{s,K}$. With regards to the induction step, we have added more detail in line with what the reviewer suggested. When deducing the upper bound of $C_s(X)$, the cardinality of L is $|L| = s$. Hence, the constant that appears in the second equation is actually a new constant that depends on s. With the suggested notation, reenumerating the constants as they change, we believe this step will be clearer, but let us know if there are still any further questions about this proof.

2. Lemma 4.4. We agree with the clarification suggested, and have rephrased the statement accordingly.

3. Remark 4.6. The coefficient $25b$ was a typo, and should be $5b$, as suggested. The argument is straightforward with this modification.

We would like to thank the reviewer for the concerns raised because it made us realize that some steps were not clear enough, in particular some proofs from Section 5. In the new version of the manuscript we will add some steps to facilitate its reading and comprehension.

Review #94B

Regarding context and applications: many current blockchain projects use SNARKs, both for anonymity and scalability purposes. Unbounded recursive composition of SNARKs has been proposed to achieve succinct blockchains (eprint 2020/352). The situation is different depending on the type of SNARK used.

If one uses a SNARK that does not require pairings, suitable cycles are relatively easy to find. The downside is that such SNARKs are less efficient than pairing-based ones: pairing-based SNARK have the advantage of a verification algorithm that runs in time constant in the size of the statement being proven.

However, only the MNT pairing-friendly cycles are known, which are inefficient due to the low security provided. Some concrete examples can be seen at https://members.loria.fr/AGuillevic/pairing-friendly-curves/. An alternative is to not use cycles, but then we incur into non-native arithmetic simulation, which is another soure of inefficiency. This situation leaves us with no ideal case, which motivates the research of our paper.

Review #94C

1. Algorithm on page 8. We were not aware of some of these results, and we thank the reviewer for bringing them to our attention. Upon reading the provided papers, we agree with the reviewer that, for the case $\deg t = 2$ ($\varphi(k) \leq 4$), all the good polynomials have been identified, and thus our search algorithm seems to be futile. We will consider whether the condition given by Proposition 2.12 is still relevant, and otherwise remove the section from the manuscript.

2. Section 5. We agree that this section feels a bit disconnected from the rest of the document. The goal here was to look at pairing-friendly cycles from a different angle: whilst most of the paper has a more algebraic treatment of cycles, this section is concerned with their density. The contribution here is to quantify to some extent the folklore notion that 'pairing-friendly cycles are hard to find'.

3. Function `is_integer_valued()` in appendix C3. We follow [20, Definitions 2.6 and 2.7] and focus on polynomials that take integer values for any x in `ZZ`. Our purpose is to apply our test to known pairing-friendly families of prime order, and all of them are defined by polynomials in `ZZ[X]`. Thus, in our case this notion is enough to obtain our main result. Still, if a new family were to appear, represented by polynomials such that, for example, take integer values only when $X = a \mod n$, we could evaluate the polynomials at $nX + a$, which would yield integer-valued polynomials without losing potential curves in the transformation (the other values do not give integer parameters anyway), and work with those.

Differences between Eurocrypt'23 and Crypto'23 manuscript submissions

The main differences between the two manuscripts are the following. On the one hand, we refined the narrative to highlight the importance of our results and the context in which they are framed. On the other hand, we removed the algorithm for searching new parametric families from Section 2.2. Following the reviewers' suggestions, we also rewrote some results to make them clearer, especially Lemma 4.4 and several results in Section 5. Additionally, we improved the bounds from Corollary 4.8. Finally, we added more details to the proofs of Section 5 and give some intuition on the strategy followed to derive Theorem 5.2, which we believe facilitate the reading and comprehension of the section.

Revisiting cycles of pairing-friendly elliptic curves

No Author Given

No Institute Given

Abstract. A recent area of interest in cryptography is recursive composition of proof systems. One of the approaches to make recursive composition efficient involves cycles of pairing-friendly elliptic curves of prime order. However, known constructions have very low embedding degrees~~, hence requiring~~ . This entails large parameter sizes, which makes the overall system inefficient. In this paper, we explore 2-cycles composed of curves from families parameterized by polynomials, and show that such cycles do not exist unless a strong condition holds. As a consequence, we prove that no 2-cycles can arise from the known families, except for ~~the one that is~~ those cycles already known. Additionally, we show some general properties about cycles, and provide a detailed computation on the density of pairing-friendly cycles among all cycles.

1 Introduction

A *proof system* is interactive protocol between two parties, called the *prover* and the *verifier*. The prover aims to convince the verifier of the truth of a certain statement u, which is an element of a language $\mathcal{L}$ in NP. Associated to a statement is a *witness*, which is a potentially secret input w that the prover uses to produce the proof of $u \in \mathcal{L}$. A recent area of interest is *recursive composition* of proof systems [47,8]~~. Here~~, since it leads to *proof-carrying data (PCD)* [15], a cryptographic primitive that allows multiple untrusted parties to collaborate on a computation that runs indefinitely, and has found multiple applications [16,39,31,10]. In recursive composition of proof systems, each prover in a sequence of provers takes the previous proof and verifies it, and performs some computations on their own, finally producing a proof that guarantees that (a) the previous proof verifies correctly, and (b) the new computation has been performed correctly. This way, the verifier, who simply verifies the last proof produced in the sequence, can be sure of the correct computation of every step.

~~For recursive composition, we~~ We require two things from the proof system for recursive composition to work. First, that it is expressive enough to be able to accept its own verification algorithm as something to prove statements about, and second, that the verification algorithm is small enough so that the prover algorithm does not grow on each step. In the literature we can find several proof systems that differ on their cryptographic assumptions and performance. *Succinct non-interactive arguments of knowledge* (SNARKs) are of particular interest, since they provide a computationally sound proof of small size compared to the size of the statement [9]. In particular, we focus on pairing-based SNARKs [40,27,25], which make use of elliptic-curve pairings for verification of proofs, achieving verification time that does not depend on the size of the statement being proven. One downside of SNARKs is that they require a set of public parameters,

Authors are listed in alphabetical order (`https://www.ams.org/profession/leaders/CultureStatement04.pdf`).

known as the *common reference string (CRS)*, that is at best linear in the size of the statement. We note that there is a way to achieve recursive composition with a linear-time verifier, as long as the proof system is compatible with an efficient accumulator scheme [11,12]. However, we focus on the case of pairing-based SNARKs, due to the appeal of ~~constant-time verification~~ constant verification time.

1.1 Avoiding non-native arithmetic with cycles

~~Any~~ A pairing-based ~~SNARKs~~ SNARK relies on an elliptic curve $E/\mathbb{F}_q$ for some prime q, and such that $E(\mathbb{F}_q)$ has a large subgroup of prime order p. With this setting, the SNARK is able to prove satisfiability of arithmetic circuits over $\mathbb{F}_p$. However, the proof will be composed of elements in $\mathbb{F}_p$ and, crucially, elements in $E(\mathbb{F}_q)$. Each of these latter elements, although they belong to a group of order p, are represented as a pair of elements in $\mathbb{F}_q$. Moreover, the verification involves operations on the curve, which have formulas that use $\mathbb{F}_q$-arithmetic. Therefore, recursive composition of SNARK proofs requires to write the $\mathbb{F}_q$-arithmetic, derived from the verification algorithm, with an $\mathbb{F}_p$-circuit. ~~Ideally, we would like $q = p$. However, there is a linear-time algorithm for solving the discrete logarithm problem on curves of this kind [45]. Therefore, we shall assume that $p \neq q$.~~

Since $\mathbb{F}_p$-circuit satisfiability is an NP complete problem, it is possible to simulate $\mathbb{F}_q$-arithmetic via $\mathbb{F}_p$-operations, but this solution incurs into an efficiency blowup of $O(\log q)$ compared to native arithmetic [8, Section 3.1].

Ideally, we would like $q = p$. However, there is a linear-time algorithm for solving the discrete logarithm problem on curves of this kind [45]. Therefore, we shall assume that $p \neq q$. ~~Another~~ In this case, one approach is to instantiate a new copy of the SNARK with another elliptic curve E' to deal with $\mathbb{F}_q$-circuits. In [17], the authors propose to use a *2–chain* of pairing-friendly elliptic curves to achieve bounded recursive proof composition. A 2-chain of (pairing-friendly) elliptic curves is a tuple of pairing-friendly elliptic curves (E_1, E_2), defined over $\mathbb{F}_{p_1}$ and $\mathbb{F}_{p_2}$, where $\cancel{p_1 | \#E_2(\mathbb{F}_{p_2})}$ $p_1 \mid \#E_2(\mathbb{F}_{p_2})$.

A more ambitious approach, proposed in [8], is to use pairs of curves that also satisfy that $\cancel{\#E_2(\mathbb{F}_{p_2}) = p_1}$ $p_2 \mid \#E_1(\mathbb{F}_{p_1})$. In this case, the pair of curves is called a *2–cycle*. By alternating the instantiation of the SNARK with the two curves of the cycle, it is possible to allow unbounded recursive composition of the SNARK without incurring into non-native arithmetic simulation. Although this idea can also be used with longer cycles, 2-cycles are the optimal choice for recursive SNARKs, because they only require the generation and maintenance of two CRS.

1.2 State of the art

Silverman and Stange [44] introduced and did a systematic study on 2-cycles of elliptic curves. As they show in their paper, in general, cycles of elliptic curves are easy to find. However, for recursive ~~SNARK composition~~ composition of pairing-based SNARKs, we need to be able to compute a pairing operation on the curves of the cycle. For this reason, curves need to have a *low* embedding degree, so that the pairing can be computed in a reasonable amount of time. Such curves are called *pairing-friendly* curves.

In [14], ~~the authors~~ Chiesa, Chua, and Weidner focused on cycles of pairing-friendly curves. In particular, they showed that only prime-order curves can form cycles. The only known method to produce prime-order curves is via families of curves parameterized by polynomials, and currently there are only five that are known. The first three of these families were introduced by Miyaji, Nakabayashi, and Takano [37], who characterized all prime-order curves with embedding degrees 3, 4, and 6. These are called MNT curves. Based on the work from [26], Barreto and Naehrig [6] found a new family of curves with embedding degree 12, and later Freeman [21] found another one with embedding degree 10. The only known cycles are formed by alternating ~~Miyaji–Nakabayashi–Takano (MNT)~~ MNT curves of embedding degrees 4 and 6 [29,14]. As proposed in [8], these cycles can be used to instantiate recursive composition of SNARKs, but due to their very low embedding degree, the parameter sizes need to be very large to avoid classical discrete-logarithm attacks [35], making the whole construction slow. Furthermore, the fact that the embedding degrees are different leads to an unbalance in the parameters, making one curve larger than necessary. Therefore, it would be desirable to have 2-cycles in which both curves have the same embedding degree k, for k a bit larger than in MNT curves. For instance, [14] suggests embedding degrees 12 or 20. This would allow for more efficient instantiations of protocols that make use of recursive composition of pairing-friendly SNARKs.

~~Chiesa, Chua, and Weidner [14] characterized all the possibilities for~~ A characterization of all the possible cycles consisting of MNT curves ~~and~~ is given in [14]. They also showed that there are no cycles consisting of curves from only the Freeman or Barreto–Naehrig (BN) families. They also gave some properties and impossibility results about pairing-friendly cycles, suggesting that adding the condition of pairing-friendliness to the curves of a cycle is a strong requirement: while cycles of curves are easy to find, cycles of pairing-friendly curves are not.

Recent progress has focused on chains of elliptic curves [20] but there are still some interesting problems in the direction of cycles. In particular, [14] lists some open problems, such as studying 2-cycles where the two curves have same embedding degree or finding a cycle by combining curves from different families.

1.3 Contributions and organization

In this paper, we continue with the line of research of [14] and tackle some of the open problems suggested by the authors. In Section 2, we review the background material on elliptic curves, focusing on families of pairing-friendly curves with prime order. In Section 3, we recall the notion of cycles of elliptic curves, and what is known about them. We also present some new results, in particular a lower bound on the trace of curves involved in a 2-cycle, when both curves have the same (small) embedding degree. In Section 4 we study whether a combination of curves from different families can form a 2-cycle. This answers one of the open questions from [14], for the case of 2-cycles.

Theorem 4.5 (informal). *Parametric families either form* 2*-cycles as polynomials or only form finitely many pairing-friendly* 2*-cycles, and these can be explicitly bounded.*

Moreover, we show that no curve from any of the known families can be in a 2-cycle in which the other curve has embedding degree ~~$k \leq 20$~~ $\ell \leq 22$, even going a bit further in some cases. This is achieved by combining the previous theorem with explicit computations for each of the families. These results shed some light over the difficulty of finding new cycles of elliptic curves, considering the fact that polynomial families are the only known way to produce pairing-friendly elliptic curves with prime order. Finally, in Section 5 we estimate the density of pairing-friendly cycles among all cycles. In [4], Balasubramanian and Koblitz estimated the density of pairing-friendly curves. We generalize their result to cycles of pairing-friendly curves. We conclude the paper in Section 6. Appendices A, B, C include additional computations and SageMath code, which can also be found in [1].

2 Pairing-friendly elliptic curves

Notation. Throughout this document, we assume that $p, q, q_i > 3$ ~~and~~ are prime numbers. We denote by $\mathbb{F}_q$ the finite field with q elements. For $n \in \mathbb{N}$, we denote by ~~ζ_n an n-th primitive root of unity. We denote by~~ $\varphi(n)$ the Euler's totient function on n~~. We denote~~, and by Φ_n the n-th cyclotomic polynomial, which has degree $\varphi(n)$. A polynomial $g \in \mathbb{Q}[X]$ is *integer-valued* if $g(x) \in \mathbb{Z}$ for all $x \in \mathbb{Z}$.

2.1 Elliptic curves

An *elliptic curve* E over $\mathbb{F}_q$ (denoted $E/\mathbb{F}_q$) is a smooth algebraic curve of genus 1, defined by the equation

$$Y^2 = X^3 + aX + b,$$

for some $a, b \in \mathbb{F}_q$ such that $4a^3 - 27b^2 \neq 0$. We denote the group of $\mathbb{F}_q$-rational points by $E(\mathbb{F}_q)$, and refer to $\#E(\mathbb{F}_q)$ as the *order* of the curve. The neutral point is denoted by O. Given $m \in \mathbb{N}$, the *m-torsion group* of E is $E[m] = \{P \in E(\overline{\mathbb{F}}_q) \mid mP = O\}$, where $\overline{\mathbb{F}}_q$ is the algebraic closure of $\mathbb{F}_q$. When $q \nmid m$, we have that $E[m] \cong \mathbb{Z}_m \times \mathbb{Z}_m$. The *trace of Frobenius* (often called just *trace*) of E is

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

Hasse's theorem [43, Theorem V.1.1] states that $|t| \leq 2\sqrt{q}$, and Deuring's theorem [18, Theorem 14.18] states that, for any $t \in \mathbb{Z}$ within the Hasse bound, there exists an elliptic curve $E/\mathbb{F}_q$ with trace t.

A curve is said to be *supersingular* when $q \mid t$, and *ordinary* otherwise. Since we work with $q > 3$ prime, the Hasse bound implies that the only supersingular curves are those with $t = 0$. In the case of ordinary curves, the endomorphism ring will be an order $\mathcal{O} \subseteq \mathbb{Q}(\sqrt{d})$, where d is the square-free part of $t^2 - 4q$. The value d is called the *discriminant* of the curve E, and we say that E has *complex multiplication* by $\mathcal{O}$. Note that the Hasse bound implies that $d < 0$.[1]

Pairings and the embedding degree. Let $E/\mathbb{F}_q$ be an elliptic curve. Then, for m such that $q \nmid m$, we can build a *pairing*

$$e : E[m] \times E[m] \to \mu_m,$$

where $E[m] \cong \mathbb{Z}_m \times \mathbb{Z}_m$ is the m-torsion group of the curve and μ_m is the group of mth roots of unity. The map e is bilinear, i.e. $e(aP, bQ) = e(P, Q)^{ab}$ for any $P, Q \in E[m]$. Various instantiations of this map exist, e.g. the Weil ~~[43, §III.8] pairing~~pairing [43, §III.8]

[1] Other works take $|d|$ as the discriminant.

. Since $\mu_m \subset \mathbb{F}_{q^k}^*$ for some $k \in \mathbb{N}$ and is a multiplicative subgroup, it follows that $m \mid q^k - 1$. The smallest k satisfying this property is called the *embedding degree* of $E[m]$. When $m = \#E(\mathbb{F}_q)$, we refer to this k as the embedding degree of E.

Proposition 2.1. *Let $E/\mathbb{F}_q$ be an elliptic curve of prime order p. The following conditions are equivalent:*

- *E has embedding degree k.*
- *k is minimal such that $p \mid \Phi_k(q)$ [37, Remark 1].*
- *k is minimal such that $p \mid \Phi_k(t-1)$ [5, Lemma 1].*

Most curves have a very large embedding degree. This has a direct impact on the computational cost of computing the pairing. On the one hand, we want small embedding degrees to ensure efficient arithmetic. On the other hand, however, small embedding degrees open an avenue for attacks, more precisely the [35] and [24] reductions~~, which~~. These translate the discrete logarithm problem on the curve to the discrete logarithm problem on the finite field $\mathbb{F}_{q^k}$, where faster (subexponential) algorithms are known. With a small embedding degree, we are forced to counteract the reduction to finite field discrete logarithms by increasing our parameter sizes. Therefore, a balanced embedding degree is ~~often~~ preferred when using pairing-friendly curves.

We note the following result, useful for finding curves with small embedding degree.

Proposition 2.2. *Let $E/\mathbb{F}_q$ be an elliptic curve with prime order p and embedding degree k such that $p \nmid k$. Then $p \equiv 1 \pmod{k}$.*

Proof. The embedding degree condition is equivalent to k being minimal such that $q^k \equiv 1 \pmod{p}$. Since p is prime, by Lagrange's theorem ~~,~~ we have that $k \mid p - 1$. □

The complex multiplication (CM) method. Let $E/\mathbb{F}_q$ be an elliptic curve with prime order p and trace t. The embedding degree condition is determined by p and q alone, so the actual coefficients of the curve equation do not play any role. Because of this, the main approach to finding pairing-friendly curves tries to find (t, p, q) first, and then curve coefficients that are compatible with these values.

Given (t, p, q) such that $p = q + 1 - t$ and $t \leq 2\sqrt{q}$, Deuring's theorem ensures that a curve exists, but that does not mean that it is easy to find. The algorithm that takes (t, p, q) and produces the curve coefficients is known as the *complex multiplication (CM) method*, and its complexity strongly depends on the discriminant d of the curve. Currently, this is considered feasible up to $|d| \approx 10^{16}$ [46].

Because of our focus on finding *good* triples (t, p, q), we will identify curves with them. That is, we write $E \leftrightarrow (t, p, q)$ as shorthand for an elliptic curve $E/\mathbb{F}_q$ with order p and trace t. This curve might not be unique, but any of them will have the same embedding degree and discriminant, so they are indistinguishable for our purposes.

2.2 Pairing-friendly polynomial families

The idea of considering families of elliptic curves parameterized by low-degree polynomials is already present in [37,6], but is studied in a more systematic way in [21,23]. We will consider triples of polynomials $(t, p, q) \in \mathbb{Q}[X]^3$ such that, given $x \in \mathbb{Z}$, there is an elliptic curve $E \leftrightarrow (t(x), p(x), q(x))$.

We are interested in prime-order elliptic curves, so we require that the polynomials p, q represent primes.

Definition 2.3. *Let $g \in \mathbb{Q}[X]$. We say that g* represents primes *if:*

- *$g(X)$ is irreducible, non-constant and has a positive leading coefficient,*
- *$g(x) \in \mathbb{Z}$ for some $x \in \mathbb{Z}$ (equivalently, for infinitely many such x), and*
- *$\gcd\{g(x) \mid x, g(x) \in \mathbb{Z}\} = 1$.*

The Bunyakovsky conjecture [41] states that a polynomial in the conditions of the definition above takes prime values for infinitely many $x \in \mathbb{Z}$. We now formally define polynomial families of pairing-friendly elliptic curves.

Definition 2.4. *Let $k, d \in \mathbb{Z}$ with $d < 0 < k$. We say that a triple of polynomials $(t, p, q) \in \mathbb{Q}[X]^3$* parameterizes a family of elliptic curves *with embedding degree k and discriminant d if:*

1. *$p(X) = q(X) + 1 - t(X)$,*
2. *p is integer-valued (even if its coefficients are in $\mathbb{Q} \setminus \mathbb{Z}$),*
3. *p and q represent primes,*
4. *$p(X) \mid \Phi_k(t(X) - 1)$, and*
5. *the equation $4q(X) = t(X)^2 + |d|Y^2$ has infinitely-many integer solutions (x, y).*

We naturally extend the notation $E \leftrightarrow (t, p, q)$ to polynomial families.

Conditions 1-3 ensure that the polynomials represent infinitely many sets of parameters compatible with an elliptic curve. Condition 4 ensures that the embedding degree is at most k, where ideally k is small. Condition 5 ensures that there are infinitely many curves in the family with the same discriminant d. If this d is not too large, we will be able to use the CM method to find the curves corresponding to these parameters. If we ignore condition 5, such families are not too hard to find, as illustrated by the following lemma.[2]

Lemma 2.5. *For any integer $k \geq 3$ there are infinitely many pairs (q, E_q) with embedding degree k, and such that $|E(\mathbb{F}_q)|$ is prime, under the Bunyakovsky conjecture.*

Proof. Infinite families are known for $k = 3, 4, 6$, as detailed below in Table 2. We can then assume $\varphi(k) \geq 4$. We will construct a family represented by the polynomial tuple (t, p, q) as follows.

Let $p(X) = \Phi_{rk}(X)$, for some prime number r such that $r \nmid k$. Then, it holds that $\varphi(kr) \geq 4(r-1) \geq 2r$. We set $q = p + x^r$. Then

$$p \mid x^{rk} - 1 = (x^r)^k - 1 = (q - p)^k - 1,$$

so $p \mid q^k - 1$. In this case $p = q - x^r$, so the trace is given by $t = 1 + x^r$, and $\deg(t) \leq \deg(p)/2$. Also, the cyclotomic polynomial is irreducible, so it represents infinitely many prime values. $\square$

[2] Furthermore, numerical experiments easily find many tuples (t, p, q) with low degree and small coefficients satisfying conditions 1-4, but unfortunately not condition 5.

Let $f(X) = 4q(X) - t(X)^2$. Freeman [21] observed that condition 5 in Definition 2.4 is strongly related to the form of this polynomial.

Proposition 2.6. *Fix $k \in \mathbb{N}$, and let $(t, p, q) \in \mathbb{Z}[X]^3$ satisfying conditions (1-4) in the previous definition. Assume that one of these holds:*

- *$f(X) = aX^2 + bX + c$, with $a, b, c \in \mathbb{Z}$, $a > 0$ and $b^2 - 4ac \neq 0$. There exists a discriminant d such that ad is not a square. Also, the CM equation has an integer solution.*
- *$f(X) = (\ell X + |d|)g(X)^2$ for some discriminant d, $\ell \in \mathbb{Z}$, and $g \in \mathbb{Z}[X]$.*

Then, we have that (t, p, q) parameterizes a family of elliptic curves with embedding degree k and discriminant d.

On the other hand, if $\deg f \geq 3$, it is unlikely to produce a family of curves, as highlighted by the following result, which is a direct consequence of Siegel's theorem [43, Corollary IX.3.2.2].

Proposition 2.7. *Fix $k \in \mathbb{N}$, and let (t, p, q) as above, and satisfying conditions (1-4) in the previous definition. Assume that $f(X)$ is square-free and $\deg f \geq 3$. Then (t, p, q) cannot represent a family of elliptic curves with embedding degree k.*

Finally, [21] also ~~presents~~ proves some results on the relations between the degrees of the polynomials involved in representing a family of curves.

Proposition 2.8. *Let $t \in \mathbb{Q}[X]$. Then, for any k and any irreducible factor $\cancel{p \mid \Phi_k \circ t}$ $p \mid \Phi_k(t-1)$, we have that $\varphi(k) \mid \deg p$.*

Proposition 2.9. *Let (t, p, q) represent a family of curves with embedding degree k, with $\varphi(k) \geq 4$. If $f = 4q - t^2$ is square-free, then:*

- $\deg p = \deg q = 2 \deg t$.
- *If a is the leading coefficient of $t(X)$, then $a^2/4$ is the leading coefficient of $p(X), q(X)$.*

Known pairing-friendly families with prime order. Only a few polynomial families of elliptic curves with prime order and low embedding degree are known. The first work in this direction is due to Miyaji, Nakabayashi, and Takano, [37], who characterized all prime-order curves with embedding degrees $k = 3, 4, 6$ (these correspond to $\varphi(k) = 2$). Based on the work of Galbraith, McKee and Valença [26], two additional families were found: Barreto and Naehrig [6] found a family with $k = 12$, and Freeman [21] found another one with $k = 10$ (both cases have $\varphi(k) = 4$). Note, however, that their results are not exhaustive, meaning that there could still be other families with these embedding degrees that have not been found, unlike in the MNT case. We summarize the polynomial descriptions of these families in Table 2.

Family	k	$t(X)$	$p(X)$	$q(X)$
MNT3	3	$6X-1$	$12X^2-6X+1$	$12X^2-1$
MNT4	4	$-X$	X^2+2X+2	X^2+X+1
MNT6	6	$2X+1$	$4X^2-2X+1$	$4X^2+1$
Freeman	10	$10X^2+5X+3$	$25X^4+25X^3+15X^2+5X+1$	$25X^4+25X^3+25X^2+10X+3$
BN	12	$6X^2+1$	$36X^4+36X^3+18X^2+6X+1$	$36X^4+36X^3+24X^2+6X+1$

Table 1. Polynomial descriptions of MNT, Freeman and BN curves, where k corresponds to the embedding degree, $t(X)$ is the trace, $p(X)$ is the order, and $q(X)$ is the order of the base field.

For completeness, we note that there are no elliptic curves with prime order and embedding degree $k \leq 2$, except for a few cases of no cryptographic interest.

Proposition 2.10. *Let $p, q \in \mathbb{Z}$ be prime numbers. If $q \geq 14$, then there is no elliptic curve $E/\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = p$ and embedding degree $k \leq 2$.*

Proof. Suppose that such a curve exists.

- If $k = 1$, then $p \mid q-1$. Clearly $p \neq q-1$, since otherwise p, q cannot both be prime. Then $p \leq \frac{q-1}{2}$, and then $q - p \geq \frac{q+1}{2}$. But, at the same time, $q - p = t - 1 \leq 2\sqrt{q} - 1$, due to the Hasse bound. These two conditions are only compatible when $q \leq 9$, which is already ruled out by hypothesis.
- If $k = 2$, then $p \mid q^2 - 1 = (q-1)(q+1)$. We have that $p \nmid q - 1$ (otherwise $k = 1$), and thus $p \mid q+1$ because p is prime. Again, $p \neq q+1$, because otherwise p, q cannot both be prime. Then $p \leq \frac{q+1}{2}$, and thus $q - p \geq \frac{q-1}{2}$. By the Hasse bound, $q - p \leq 2\sqrt{q} - 1$, and these are only compatible for $q < 14$.

□

~~**An attempt at finding new families.** This section describes a technique for searching for new parametric families of pairing-friendly curves with prime order. The idea was already known to Freeman [22], although we present a new speed-up when $\deg t = 2$. Unfortunately, we cannot report any new findings, but still outline the technique due to its potential independent interest.~~

~~The algorithm works as follows: we are looking for tuples $(t, p, q) \in \mathbb{Q}[X]^3$ in the conditions of Definition 2.4. We first note that the three polynomials are in the linear relation $p = q + 1 - t$, so we actually just need to find two of them. Moreover, by Proposition 2.1, we know that p is limited to the irreducible factors of $\Phi_k(q)$ or $\Phi_k(t-1)$, so if we have one of these, then we will have very few candidates for p. We use $t - 1$ as our "free" polynomial because it has lower degree than q.~~

~~$d = \varphi(k)/2$ $t = \sum_{i=0}^{d} t_i X^i$ $q = p - 1 + t$ **continue** $f = 4q - t^2$ **continue** **print** (t, p, q)~~

~~We present a way to speed up this search when $\deg t = 2$, based on the following result.~~

~~Let $t \in \mathbb{Q}[X]$ with $\deg t = 2$. Then:~~

- ~~If $t(X) = \zeta_k$ has a solution in $\mathbb{Q}(\zeta_k)$, then $\Phi_k \circ t$ factors over the rationals into two irreducible polynomials of degree $\varphi(k)$ each.~~

– ~~Otherwise, $\Phi_k \circ t$ is irreducible and has degree $2\varphi(k)$.~~

~~The proposition below allows us to replace the brute force in the three coefficients (t_0, t_1, t_2) of t by the leading coefficient and discriminant, (t_2, Δ).~~

~~Let $a, b, c, k \in \mathbb{Z}$, with $a \neq 0$ and $k \geq 3$. Consider the polynomial $t(X) = aX^2 + bX + c$ with discriminant Δ. If $t(X) = \zeta_k$ has a solution in $\mathbb{Q}(\zeta_k)$, then $\Phi_k\left(-\frac{\Delta^2}{4a}\right)$ is a square in $\mathbb{Q}$.~~

~~We have~~

$$4at(X) = (2aX + b)^2 - \Delta^2,$$

~~where $\Delta = \sqrt{b^2 - 4ac}$ is the discriminant of the polynomial $t(X)$. Hence, we are looking for solutions of the equation~~

$$y^2 - \Delta^2 = 4a\zeta$$

~~over $K = \mathbb{Q}(\zeta)$. Raising Equation to the k-th power, we get~~

$$0 = \left(y^2 - \Delta^2\right)^k - (4a)^k = y^{2k} + \sum_{j=1}^{k} \binom{k}{j} (-1)^j y^{2k-2j} \left(\Delta^2\right)^j .$$

~~In particular, y is a root of a monic polynomial with integer coefficients, and hence, it is an algebraic integer. Taking norms in K we get~~

$$N(y)^2 = \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \left(\Delta^2 + 4a\sigma(\zeta)\right) = (4a)^{\varphi(k)} \Phi_k\left(-\frac{\Delta^2}{4a}\right).$$

~~If Equation does not have a solution over the integers, then neither does $t(X) = \zeta_k$. Since the norm of an algebraic integer is an integer and $2 | \varphi(k)$ for $k \geq 3$, then $\Phi_k\left(-\frac{\Delta^2}{4a}\right)$ must be a square.~~

~~The idea is the same as outlined in the algorithm above, but now we loop over (t_2, Δ) instead of (t_0, t_1, t_2), and proceed only if $\Phi_k(-\frac{\Delta^2}{4a})$ is a square. Since the condition is necessary but not sufficient, we still need to check for irreducibility of $\Phi_k(t-1)$. Once a suitable pair (t_2, Δ) has been found, we look for t_1, t_0 compatible with Δ. Still, this was not enough to find any new instances of families for the values of k compatible with $\deg t = 2$, that is, $5, 8, 10, 12$ (those with $\varphi(k) = 4$).~~

3 Cycles of elliptic curves

3.1 Definition and known results

The notion of cycles of elliptic curves was introduced in [44].

Definition 3.1. *Let $s \in \mathbb{N}$. An* s-cycle of elliptic curves *is a tuple $(E_1, \ldots, E_s)$ of elliptic curves, defined over fields $\mathbb{F}_{q_1}, \ldots, \mathbb{F}_{q_s}$, respectively, and such that*

$$\#E_i(\mathbb{F}_{q_i}) = q_{i+1 \bmod s},$$

for all $i = 1, \ldots, s$.

Remark 3.2. Cycles of length 2 have some particular properties that are worth noting. Let E, E' be two curves forming a 2-cycle. ~~Then~~

- If $E \leftrightarrow (t, p, q)$, then Definition 3.1 implies that $E' \leftrightarrow (2 - t, q, p)$.
- ~~E~~ We have that $p = \#E(\mathbb{F}_q)$ is in the Hasse interval of ~~E'~~ $q = \#E'(\mathbb{F}_p)$ if and only if ~~E'~~ q is in the Hasse interval of ~~E~~ p. Indeed, if the former holds, ~~we have that~~ then

  $$\sqrt{p} - 1 \leq \sqrt{q} \leq \sqrt{p} + 1,$$

  which is equivalent to

  $$\sqrt{q} - 1 \leq \sqrt{p} \leq \sqrt{q} + 1.$$

It is known that cycles of any length exist [44, Theorem 11]. We summarize in the following two propositions some facts about cycles. These results are due to [14].

Proposition 3.3. *Let $E_1, \dots, E_s$ be an s-cycle of elliptic curves, defined over prime fields $\mathbb{F}_{q_1}, \dots, \mathbb{F}_{q_s}$. Then:*

(i) *$E_1, \dots, E_s$ are ordinary curves.*
(ii) *If $q_1, \dots, q_s > 12s^2$, then $E_1, \dots E_s$ have prime order.*
(iii) *Let $t_1, \dots, t_s$ be the traces of $E_1, \dots, E_s$, respectively. Then*

$$\sum_{i=1}^{s} t_i = s.$$

(iv) *If $s = 2$, then the curves in the cycle have the same discriminant d.*
(v) *If the curves in the cycle have the same discriminant $|d| > 3$, then $s = 2$.*
(vi) *If $s > 2$ and $E_1, \dots, E_s$ have the same discriminant d, then necessarily $s = 6$ and $|d| = 3$.*

There are also some impossibility results.

Proposition 3.4. *We have the following.*

(i) *There ~~do not exist~~ is no 2~~-cycles~~-cycle with embedding degree pairs $(5, 10)$, $(8, 8)$ or $(12, 12)$.*
(ii) *There ~~do not exist cycles~~ is no cycle formed only by Freeman curves.*
(iii) *There ~~do not exist cycles~~ is no cycle formed only by BN curves.*

3.2 Some properties of cycles

In this section, we show some results about cycles, most of them about 2-cycles in which both curves have the same embedding degree.

Proposition 3.5. *~~Sophie Germain~~ Safe primes are not part of any 2-cycle in which both curves have the same embedding degree k.*

Proof. Let p, q be the orders of the curves in the cycle~~, and assume that one of them is a Sophie Germain prime. Let us say $p = 1 + 2\ell$, with ℓ~~. Assume that p is a safe prime, i.e. $p = 1 + 2r$, with r prime. Since ~~they~~ p, q are in a cycle, $q = p + 1 - t$ for some $|t| \leq 2\sqrt{p}$. Now, since $k \mid p - 1$ by Proposition 2.2, we have $\cancel{k = 1, 2, \ell, 2\ell}$ $k = 1, 2, r, 2r$. We already know that $k \neq 1, 2$~~. Hence, $k = \ell$ or 2ℓ~~, hence $k \in \{r, 2r\}$. But then $\cancel{\ell \mid q - p}$ $r \mid q - p$, and thus

$$|q - p| \geq \cancel{\ell} r = \cancel{(p-1)/2} \frac{p - 1}{2} > 2\sqrt{p} + 1$$

for any $\cancel{p > 3}$ $p > 3$, which contradicts the fact that $\cancel{|q - p| = |1 - t| \leq 2\sqrt{p} + 1.}$ $|q - p| = |1 - t| \leq 2\sqrt{p} + 1$. ∎

Proposition 3.6. *Let $s \in \mathbb{Z}$~~. Consider~~ , and let $(t, p, q) \in \mathbb{Q}[X]^3$ parameterize a family of ~~elliptic curves with trace parameterized by a polynomial $t \in \mathbb{Q}[X]$~~ pairing-friendly elliptic curves, with $\deg t$ even. Then, there are only finitely many ~~curves from this family form~~ s-cycles ~~within~~ such that all s curves in the cycle belong to the family.*

Proof. If s curves with traces $t_1, \ldots, t_s$, respectively, form a cycle, by Proposition 3.3.(iii) we have that $\sum_{i=1}^{s} t_i = s$. Since $\deg t \geq 2$ and s is fixed, necessarily there exist $a, b \in \{1, \ldots, s\}$ such that t_a, t_b have different signs. However, since $\deg t$ is even, there exists a lower bound b such that, for all $|x| > b$, we have that $t(x)$ has the same sign. Therefore, only finitely many cases can occur in which the traces have opposing sign. ∎

Given an elliptic curve $E \leftrightarrow (t, p, q)$, Hasse's theorem gives us the bound $|t| \leq 2\sqrt{q}$, which ~~translates to~~ in the polynomial case ~~as~~ implies that $\deg t \leq \frac{1}{2}\deg q$. We now derive a lower bound for t in the case of 2-cycles in which both curves have the same small embedding degree. We require first the following technical lemma.

Lemma 3.7. *Let $k \in \mathbb{N}$ and $3 \leq k \leq 104$. We have that:*

(i) For any $|x| > 1$,

$$\Phi_k(x) \leq \frac{|x|}{|x| - 1} x^{\varphi(k)}.$$

(ii) For any $\varepsilon > 0$, there exists $B > 0$ such that, for all x with $|x| > B$,

$$\Phi_k(x - 1) \leq (1 + \varepsilon) \frac{|x|}{|x| - 1} x^{\varphi(k)}.$$

Proof. Clearly such bound exists for $|x|$ large enough, since $\Phi_k(x) = x^{\varphi(k)} + o\left(x^{\varphi(k)}\right)$. More precisely, for $k \leq 104$, the k-th cyclotomic polynomial has only 0 and ± 1 as coefficients [36]. Therefore

$$\Phi_k(x) \leq x^{\varphi(k)} + \sum_{i=0}^{\varphi(k)-1} |x|^i = x^{\varphi(k)} \left(1 + \sum_{i=1}^{\varphi(k)} \frac{1}{|x|^i}\right) \leq x^{\varphi(k)} \left(1 + \frac{1}{|x| - 1}\right) = \frac{|x|}{|x| - 1} x^{\varphi(k)},$$

using the fact that the geometric series converges when $|x| > 1$.

Part (ii) is now trivial when $x > 0$. For $x < 0$, we note that, since Φ_k is a polynomial with positive leading coefficient, for any $\varepsilon > 0$ there exists $B > 0$ such that, for all x with $|x| > B$,

$$\Phi_k(x - 1) \leq (1 + \varepsilon)\Phi_k(x),$$

since otherwise the function would grow exponentially fast when $x \to -\infty$. The result follows directly from applying part (i) to $\Phi_k(x)$. $\square$

Remark 3.8. More precisely, for k such that $3 \leq k \leq 104$, we do not need to choose B too large to achieve a small constant. The following values have been obtained computationally.

$1+\varepsilon$	2	1.1	1.01
B	146	1069	10250

Proposition 3.9. *Let $E \leftrightarrow (t, p, q)$ be an elliptic curve with embedding degree k, with $|t| > 1$ and $3 \leq k \leq 104$. Then, for any $\varepsilon > 0$ there exists $B > 0$ such that, for all x with $|x| > B$, we have*

$$|t| > \left(\frac{1}{1+\varepsilon}\frac{|t|-1}{|t|}q\right)^{\frac{1}{\varphi(k)}}.$$

Proof. We have that $p \mid \Phi_k(t-1)$, so $p \leq \Phi_k(t-1)$. Also, we have that $|t| < |\Phi_k(t) - \Phi_k(t-1)|$. Assume first that $t > 1$. Then, due to part (i) of the previous lemma,

$$q = p - 1 + t \leq p + t < \Phi_k(t) \leq \frac{t}{t-1}t^{\varphi(k)}.$$

Taking $\varphi(k)$-th roots,

$$t > \left(\frac{t-1}{t}q\right)^{\frac{1}{\varphi(k)}}.$$

The case $t < -1$ is completely analogous, using part (ii) of Lemma 3.7. $\square$

The result above deals with a single curve, but actually it can be strengthened for some 2-cycles.

Proposition 3.10. *Let $E \leftrightarrow (t, p, q)$ and* ~~$E \leftrightarrow (2-t, q, p)$~~ $E' \leftrightarrow (2-t, q, p)$ *be two elliptic curves with $|t| > 1$ and the same embedding degree $k \equiv 0 \pmod 4$, such that* ~~$k \leq 3 \leq 104$~~$3 \leq k \leq 104$. *Then, for any $\varepsilon > 0$ there exists $B > 0$ such that, for all x with $|x| > B$, we have*

$$|t| > \left(\frac{1}{1+\varepsilon}\frac{|t|-1}{|t|}q\right)^{\frac{2}{\varphi(k)}}.$$

Proof. The case $k \equiv 0 \pmod 4$ corresponds to those cyclotomic polynomials such that $\Phi_k(x) = \Phi_k(-x)$ for all x. From the embedding degree conditions, we have

$$p \mid \Phi_k(t-1),$$
$$q \mid \Phi_k(1-t),$$

and therefore $pq \mid \Phi_k(t-1)$, since p, q are different primes. Assume, without loss of generality, that $q < p$. Then $q^2 \leq pq \leq \Phi_k(t-1)$, and proceeding as the proof of Proposition 3.9, we obtain

$$q^2 \leq (1+\varepsilon)\frac{|t|}{|t|-1}t^{\varphi(k)},$$

from which we obtain the desired bound. $\square$

Corollary 3.11. *Let $E \leftrightarrow (t,p,q)$ and ~~$E \leftrightarrow (2-t,q,p)$~~ $E' \leftrightarrow (2-t,q,p)$ be two elliptic curves with the same embedding degree $k \equiv 0 \pmod 4$, such that ~~$k \leq 3 \leq 104$~~$3 \leq k \leq 104$. There exists B such that, if $|t| > B$, then*

$$\frac{1}{2}q^{\frac{2}{\varphi(k)}} < |t| \leq 2q\frac{1}{2}.$$

Remark 3.12. The result above is particularly interesting in two cases:

– When $\varphi(k) = 2$, i.e. $k = 4$. In this case,

$$\frac{1}{2}q < |t| \leq 2q\frac{1}{2},$$

which cannot happen for $q \geq 15$. This shows that there are no $(4,4)$-cycles (which was already known from [14]).

– When $\varphi(k) = 4$, i.e. $k \in \{8, 12\}$. In this case,

$$\frac{1}{2}q\frac{1}{2} < |t| \leq 2q\frac{1}{2},$$

which shows that t asymptotically behaves like $\sqrt{q}$, and therefore is on the outermost part of the Hasse interval. In particular, for polynomial families this means that $\deg t = \frac{1}{2}\deg p$, which improves on the inequality known before~~. This is consistent with what is observed in known families~~.

4 Cycles from known families

In this section, we prove our main result about 2-cycles of elliptic curves: given a family $(t,p,q) \in \mathbb{Q}[X]^3$ with embedding degree k, and $\ell \in \mathbb{N}$, one of two things can happen:

(a) ~~$q \mid p^\ell - 1$~~$q \mid \Phi_\ell(1-t)$, as polynomials. In this case, any curve in the family forms a 2-cycle with the corresponding curve in the family $(2-t,q,p)$, which has embedding degree ℓ (see Proposition 2.1). Observe that, due to Proposition 3.3, both families have the same discriminant.

(b) Only finitely many curves from the family form a 2-cycle with curves of embedding degree ℓ.

Furthermore, when we are in the second case we can explicitly find these cycles. For all known families (Table 2), we prove that no curve from them (except for a few anecdotal cases) is part of a 2-cycle with any curve with embedding degree ~~$\ell \leq 20$~~$\ell \leq L$. The bound L depends on the family, and in all cases at least $L \geq 22$.

4.1 Cycles from parametric-families

First, we show a technique ~~will that~~ that will help us rule out many cases from our main results, by performing a very simple check.

Proposition 4.1. *Let $(t, p, q) \in \mathbb{Q}[X]^3$ parameterize a family of pairing-friendly elliptic curves~~, and let $\ell \in \mathbb{N}$ such that~~*

$$q(i) \not\equiv 1 \pmod{\ell}$$

~~for $i = 0, \ldots, \ell - 1$. Then, if~~ . Let a curve E from the family ~~is~~ be in a cycle, and assume that the previous curve in the cycle ~~does not have~~ has embedding degree ℓ. Then there exists $i \in \{0, \ldots, \ell - 1\}$ such that

$$q(i) \equiv 1 \pmod{\ell}.$$

Proof. Let $x \in \mathbb{Z}$ such that $E \leftrightarrow (t(x), p(x), q(x))$, and let $E' \leftrightarrow (t', p', q')$ be the previous curve in the cycle ~~. We assume that E' has~~ with embedding degree ℓ~~, and will reach a contradiction~~. From the definition of cycle, $p' = q(x)$. Then, applying Proposition 2.2 to curve E', we deduce that

$$q(x \bmod \ell) \equiv q(x) \equiv p' \equiv 1 \pmod{\ell}.$$

~~This contradicts the hypothesis $q(i) \not\equiv 1 \pmod{\ell}$ for $i = 0, \ldots, \ell$.~~ □

By testing the ~~property of~~ condition given by Proposition 4.1 for known families and $3 \leq \ell \leq 100$, we obtain the following results.

Corollary 4.2. *An MNT3 curve cannot be preceded in a cycle by a curve with embedding degree ℓ, where*

$$\begin{aligned} \ell \in \{&3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 15, 16, 17, 18, 20, 21, 22, 24, 26, 27, 28, 30, 31, 32, 33, 34, 35, 36, \\ &37, 39, 40, 41, 42, 44, 45, 48, 49, 51, 52, 54, 55, 56, 57, 59, 60, 61, 62, 63, 64, 65, 66, 68, 69, 70 \\ &72, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 87, 88, 89, 90, 91, 92, 93, 96, 98, 99, 100\}. \end{aligned}$$

Corollary 4.3. *A Freeman curve cannot be preceded in a cycle by a curve with embedding degree ℓ, where*

$$\begin{aligned} \ell \in \{&4, 5, 8, 10, 11, 12, 15, 16, 20, 22, 24, 25, 28, 30, 32, 33, 35, 36, 40, 44, 45, 48, 50, 52, 53, 55, 56, \\ &59, 60, 61, 64, 65, 66, 68, 70, 72, 75, 76, 77, 79, 80, 83, 84, 85, 88, 90, 92, 95, 96, 97, 99, 100\}. \end{aligned}$$

Furthermore, even when we cannot rule out a certain ℓ, we obtain a condition on $x \bmod \ell$, which will help us later when we check by brute force all x in an interval. Also note that, despite the fact that we will use these corollaries to simplify our work in the next section, which deals with 2-cycles, these results work for cycles of any length.

4.2 2-cycles from parametric families

The goal here will be to start from a known family of pairing-friendly elliptic curves, and argue that they form no 2-cycles with other pairing-friendly curves. To do so, let (t, p, q) represent such family. For any curve $E \leftrightarrow (t(x), p(x), q(x))$, there is another curve $E' \leftrightarrow (2 - t(x), q(x), p(x))$ such that the two of them form a 2-cycle. Furthermore, if E' has a small embedding degree $\ell \in \mathbb{Z}$, then $q(x) \mid p(x)^\ell - 1$. Note that this is for a particular $x \in \mathbb{Z}$, not as polynomials.

Informally, our strategy will be the following. The embedding degree condition on E' can be reformulated in terms of integer division: the division of $p(x)^\ell$ by $q(x)$ has remainder 1. We will compare integer division and polynomial division, and show that, outside of a finite interval ~~$[A, B]$~~ $[N_{\mathsf{left}}, N_{\mathsf{right}}]$, the remainders in both cases essentially agree. Therefore, by showing that the polynomial remainder $r(x)$ never takes the value 1, we will rule out any possibility of cycles outside of ~~$[A, B]$~~ $[N_{\mathsf{left}}, N_{\mathsf{right}}]$. For known families of curves, we will deal with the cases ~~$x \in [A, B]$~~ $x \in [N_{\mathsf{left}}, N_{\mathsf{right}}]$ manually, as there are only a finite number of them, and show that none of them leads to a partner curve with small embedding degree.

Lemma 4.4. *Let $x \in \mathbb{Z}$, and let $a, b \in \mathbb{Q}[X]$ be two integer-valued polynomials. Assume that b has even degree and positive leading coefficient.*

- *Let $h, r \in \mathbb{Q}[X]$ be the quotient and remainder, respectively, of the polynomial division of a by b. Let $c > 0$ be the smallest integer such that $ch, cr \in \mathbb{Z}[X]$.*
- *Let $h_x, r_x \in \mathbb{Z}$ be the quotient and remainder, respectively, of the integer division of $ca(x)$ by $b(x)$.*

Then either $\deg r = 0$, or there exist ~~$A, B \in \mathbb{Z}$ such that, for all $x \in \mathbb{Z} \setminus [A, B]$~~ $N_{\mathsf{left}}, N_{\mathsf{right}} \in \mathbb{Z}$ and $\delta_{\mathsf{left}}, \delta_{\mathsf{right}} \in \{0, 1\}$ such that:

- *For all $x < N_{\mathsf{left}}$, we have that $\operatorname{sign}(r(x))$ is constant, and $r(x) = cr(x) + \delta_{\mathsf{left}} b(x)$.*
- *For all $x > N_{\mathsf{right}}$, we have that ~~either $r_x = cr(x)$ or $r_x = cr(x) + b(x)$. More precisely~~ $\operatorname{sign}(r(x))$ is constant, and $r(x) = cr(x) + \delta_{\mathsf{right}} b(x)$.*

Furthermore, let us denote ~~$\sigma_A = \operatorname{sign}\{r(x) \mid x < A\}$ and $\sigma_B = \operatorname{sign}\{r(x) \mid x > B\}$, respectively. Then~~ $\sigma_{\mathsf{left}} = \operatorname{sign}\{r(x) \mid x < N_{\mathsf{left}}\}$ and $\sigma_{\mathsf{right}} = \operatorname{sign}\{r(x) \mid x > N_{\mathsf{right}}\}$. Then

$$\cancel{r_x}\,\delta_{\mathsf{left}} = \frac{1 - \sigma_{\mathsf{left}}}{2}, \qquad \delta_{\mathsf{right}} = \frac{1 - \sigma_{\mathsf{right}}}{2}.$$

Proof. We observe that c is well-defined, as it can be taken as the least common multiple of all denominators occurring in the coefficients of h, r. Likewise, ~~σ_A, σ_B~~ $\sigma_{\mathsf{left}}, \sigma_{\mathsf{right}}$ are well-defined, since r is a polynomial, and thus at most it changes sign $\deg r$ times. For the second part, we have that

$$\begin{aligned} ca(x) &= b(x)h_x + r_x, \\ ca(x) &= b(x)(ch(x)) + cr(x), \end{aligned}$$

where $0 \le r_x < b(x)$, and $\deg r < \deg b$, and all these values are integer. Subtracting, we obtain ~~$r_x - cr(x) = b(x)(ch(x) - h_x)$,~~

$$r_x - cr(x) = b(x)(ch(x) - h_x),$$

and thus $r_x \equiv cr(x) \pmod{b(x)}$. Since $0 \le r_x < b(x)$, we just need to find $cr(x) \bmod b(x)$, as this will necessarily ~~agree with~~ be the same as r_x.

We illustrate the technique for the case ~~$\sigma_A = -1, \sigma_B = 1$~~ $\sigma_{\mathsf{left}} = -1, \sigma_{\mathsf{right}} = 1$ (the other cases are completely analogous). Note that, if $\deg r > 0$, then r is not a constant polynomial.

– Let ~~$A \in \mathbb{Z}$~~ $N_{\text{left}} \in \mathbb{Z}$ be the largest integer such that $0 < -cr(x) \leq b(x)$ for all ~~$x < A$. Such A~~ $x < N_{\text{left}}$. Such N_{left} exists because both $b(x), -cr(x) \to \infty$ when $x \to -\infty$, and $\deg b > \deg(-cr)$. If ~~$x < A$~~$x < N_{\text{left}}$, then $0 < -cr(x) \leq b(x)$. Multiplying by (-1), we get that $-b(x) \leq cr(x) < 0$, and adding $b(x)$, we get $0 \leq cr(x) + b(x) < b(x)$. Therefore, $r_x = cr(x) + b(x)$.

– Let ~~$B \in \mathbb{Z}$~~ $N_{\text{right}} \in \mathbb{Z}$ be the smallest integer such that $0 \leq cr(x) < b(x)$ for all ~~$x > B$. Such B~~ $x > N_{\text{right}}$. Such N_{right} exists because both $b(x), cr(x) \to \infty$ when $x \to \infty$, and $\deg b > \deg(cr)$. If ~~$x > B$~~$x > N_{\text{right}}$, then $0 \leq cr(x) < b(x)$. Therefore, necessarily $r_x = cr(x)$.

□

We can now prove the main theorem of this section, from which the desired results will directly follow.

Theorem 4.5. *Let $k, \ell \in \mathbb{N}$. Let (t, p, q) be a triple of polynomials parameterizing a family of elliptic curves with embedding degree k. Then either $q \mid p^\ell - 1$ as polynomials, or there are at most finitely many 2-cycles formed by a curve from the family and a curve with embedding degree ~~k~~ℓ.*

Proof. Due to Proposition 2.10, we can safely assume that $k, \ell \geq 3$. Assume that there exists a 2-cycle involving a curve E from the family and another curve E' with embedding degree ℓ. That is, assume that there exists $x \in \mathbb{Z}$ such that $E \leftrightarrow (t(x), p(x), q(x))$ is in a 2-cycle. Then $E' \leftrightarrow (2 - t(x), q(x), p(x))$. By the condition of the embedding degree, we have that

$$q(x) \mid p(x)^\ell - 1,$$

and thus there exists $h \in \mathbb{Z}$ such that

$$p(x)^\ell = q(x)h + 1.$$

We now wish to apply Lemma 4.4, with $a = p^\ell$ and $b = q$, so we must argue that q has even degree and positive leading coefficient. We distinguish two cases:

– For $k \in \{3, 4, 6\}$, all the prime-order families are the MNT families, which have $\deg q = 2$ and positive leading coefficient.
– For k with $\varphi(k) \geq 4$, we have from Lemma 2.8 that $\varphi(k) \mid \deg p$, and in this case $\varphi(k)$ is always even. Furthermore, since $p = q + 1 - t$ and $t = O(\sqrt{q})$ (due to the Hasse bound), necessarily $\deg q = \deg p$. Now, since q has even degree, it necessarily has positive leading coefficient, otherwise it could not represent infinitely many curves.

Let $h, r \in \mathbb{Q}[X]$ be the quotient and remainder, respectively, of the polynomial division of p^ℓ by q. If $q \nmid p^\ell - 1$ as polynomials, then $r \neq 1$. If r is another constant polynomial, then the embedding degree condition does not hold for any $x \in \mathbb{Z}$. If $\deg r > 0$, Lemma 4.4 gives us ~~$c, A, B, \in \mathbb{Z}, \sigma_A, \sigma_B \in \{\pm 1\}$~~ $c, N_{\text{left}}, N_{\text{right}}, \in \mathbb{Z}, \delta_{\text{left}}, \delta_{\text{right}} \in \{0, 1\}$ such that, if ~~$x < A$,~~ $x < N_{\text{left}}$,

$$cr(x) + \cancel{\frac{1 - \sigma_A}{2}}\delta_{\text{left}} b(x) = 1,$$

and if ~~$x > B$, then~~ $x > N_{\text{right}}$, then

$$cr(x) + \cancel{\frac{1 - \sigma_B}{2}}\delta_{\text{right}} b(x) = 1.$$

The polynomials $cr(X)$ and $cr(X)+b(X)$ can only take the value 1 finitely many times. By ~~increasing A, B~~ enlarging $[N_{\mathsf{left}}, N_{\mathsf{right}}]$ if necessary, we can ensure that this only happens inside of ~~$[A, B]$~~$[N_{\mathsf{left}}, N_{\mathsf{right}}]$. Therefore, there are no cycles for ~~$x \notin [A, B]$~~$x \notin [N_{\mathsf{left}}, N_{\mathsf{right}}]$. ∎

This result immediately yields the following consequences for concrete families of curves. Let (t, p, q) parametrize a family of curves. Given a certain value of ℓ, it is immediate to check whether ~~$q \nmid \ell^k - 1$~~ $q \nmid p^\ell - 1$ as polynomials. If that is not the case (which happens most of the time), Theorem 4.5 ensures that there are at most finitely-many cycles formed by a curve from the family and a curve with embedding degree ℓ. For each candidate ℓ, we compute the values ~~c, A, B~~ $c, N_{\mathsf{left}}, N_{\mathsf{right}}$ from Theorem 4.5 corresponding to the division of p^ℓ by q. Interestingly, $c = 1$ for all known families of pairing-friendly curves with prime order. The resulting values of ~~A, B~~ $N_{\mathsf{left}}, N_{\mathsf{right}}$ are summarized in Table 3 for the MNT3, Freeman, and BN families. No tables are included for MNT4 and MNT6 families because, in these cases, we have ~~$A = -1, B = 0$ and $A = B = 0$~~$N_{\mathsf{left}} = -1, N_{\mathsf{right}} = 0$ and $N_{\mathsf{left}} = N_{\mathsf{right}} = 0$, respectively, regardless of ℓ.

Remark 4.6. Given arbitrary integer-valued polynomials $p, q \in \mathbb{Q}[X]$ and $\ell \in \mathbb{N}$, there is no guarantee that the polynomial remainder of p^ℓ by q will have integer coefficients, i.e. $c = 1$, or even be integer-valued. Nevertheless, this does happen for MNT, Freeman, and BN curves. We show this for Freeman curves, but the argument is very similar in all cases. For completeness, the other cases are included in Appendix A.

We proceed by induction on ℓ. For $\ell = 1$, we have that

$$p(X) \bmod q(X) = -10X^2 - 5X - 2.$$

This polynomial is of the form ~~$25aX^3 + 25bX^2 + 5cX + d$~~$25aX^3 + 5bX^2 + 5cX + d$, for some $a, b, c, d \in \mathbb{Z}$. We will now show that, if $p^\ell \bmod q$ is of this form, then $p^{\ell+1} \bmod q$ is also of this form. This will prove that all the remainder is actually in $\mathbb{Z}[X]$ for any $\ell \in \mathbb{N}$.

Hence, suppose that there exist $a, b, c, d \in \mathbb{N}$ such that

$$p(X)^\ell \bmod q(X) = 25aX^3 + 5bX^2 + 5cX + d.$$

Then

$$\begin{aligned} p(X)^{\ell+1} &\equiv p(X)^\ell p(X) \equiv \left(25aX^3 + 5bX^2 + 5cX + d\right)\left(-10X^2 - 5X - 2\right) \\ &\equiv -250aX^5 - (125a + 50b)X^4 - (50a + 25b + 50c)X^3 \\ &\quad -(10b + 25c + 10d)X^2 - (10c + 5d)X - 2d \\ &\equiv (75a + 25b - 50c)X^3 + (-25a + 40b - 25c - 10d)X^2 \\ &\quad +(-20a + 20b - 10c - 5d)X + (-15a + 30b - 2d) \pmod{q(X)}. \end{aligned}$$

Since the coefficient of degree 3 is divisible by 25, and the coefficients of degree 2 and 1 are divisible by 5, the induction step works.

Remark 4.7. The values of ~~A, B~~ $N_{\mathsf{left}}, N_{\mathsf{right}}$ in MNT4 and MNT6 families are in stark contrast with the other families (shown in Appendix B), but can be easily explained. In MNT3, ~~BN and Freeman~~Freeman, and BN curves, the remainder r of the polynomial division q^k by p has coefficients that mostly increase with k. Because of this, we need to get further away from zero before the asymptotic ~~behaviour~~ behavior kicks in.

On the contrary, only a small number of remainders are possible in MNT4 and MNT6 curves. Let ~~$p, q \in \mathbb{Q}[X]$ be the polynomials parameterizing the order of~~ $(t, p, q) \in \mathbb{Q}[X]^3$ parameterize MNT4 curves~~and the order of their base fields~~. We have that $q \mid p^6 - 1$ (they form infinitely many cycles with MNT6 curves). That is, p has order 6 modulo q, and thus $p^k \bmod q$ can only take 6 possible values. Concretely, $p(X)^k \bmod q(X) \in \{\pm 1, \pm X, \pm(X + 1)\}$ for any $k \in \mathbb{N}$, and all of these yield the bounds ~~$A = -1, B = 1$~~$N_{\mathsf{left}} = -1, N_{\mathsf{right}} = 0$. Similarly, in the case of MNT6 curves, the remainder of p^k by q can only take 4 values. Concretely $p(X)^k \bmod q(X) \in \{\pm 1, \pm 2X\}$ for any $k \in \mathbb{N}$, which yield the bounds ~~$A = B = 0$~~$N_{\mathsf{left}} = N_{\mathsf{right}} = 0$.

An exhaustive search in ~~$[A, B]$~~ $[N_{\mathsf{left}}, N_{\mathsf{right}}]$ reveals no curves with embedding degree ℓ, for any of the values of ℓ considered, except for a few examples with no cryptographic interest. We consider MNT3, Freeman, and BN curves, since it is already known [14] that MNT4 and MNT6 curves are only in cycles with each other.

Corollary 4.8. *Let (E, E') be a 2-cycle of elliptic curves, and assume that ~~E' has embedding degree $\ell \leq 20$~~E is not one of the curves described in Table **??**. Then:*

(i) If E is ~~not an MNT curve, unless (E, E') is a cycle formed by an MNT4-MNT6 pair~~an MNT3 curve, then E' has embedding degree $\ell \geq 23$.
(ii) If E is ~~not~~ a Freeman curve, then E' has embedding degree $\ell \geq 26$.
(iii) If E is ~~not~~ a BN curve, then E' has embedding degree $\ell \geq 33$.

Family	k	ℓ	x	t	p	q
MNT3	3	10	-1	-7	19	11
MNT3	3	10	1	5	7	11
BN	12	18	-1	7	13	19

Table 2. Instances of curves $E \leftrightarrow (t, p, q)$, with embedding degree k, from known cycles that form a pairing-friendly 2-cycle with another curve E' with embedding degree ℓ.

The computational check took a few hours on a standard computer, using the SageMath code from Appendix C. Theoretically, there is no reason to stop at a given embedding degree ℓ. However, the interval $[N_{\mathsf{left}}, N_{\mathsf{right}}]$ grow rapidly, making the brute force check inside of the interval a much more serious computing effort, requiring a more polished implementation. Still, the most interesting cases are those with smaller embedding degree, as the ideal cycles for recursive composition would be those in which the embedding degrees of both curves are as close as possible.

5 ~~Probabilities and estimates~~Density of pairing-friendly cycles

So far, this work has been mostly an algebraic treatment of cycles. In this section, we ~~generalize the results in [4]~~ look at cycles from a different angle, concerning ourselves with their density. The goal is to quantify in concrete terms the folklore notion that pairing-friendly cycles are hard to find. Our starting point is the following result of [4]. It proves an upper bound on the probability of a random elliptic curve being pairing-friendly.[3]

Theorem 5.1 ([4], Theorem 2). *Let $M \in \mathbb{Z}$. Let $\mathfrak{p}$ be the probability of finding an elliptic curve $E/\mathbb{F}_q$ with prime order $p \in [M, 2M]$ and embedding degree $k \leq (\log q)^2$, by sampling uniformly from all the curves with orders in the interval $[M, 2M]$. Then*

$$\mathfrak{p} < c\frac{(\log M)^9(\log\log M)^2}{M},$$

for some constant $c > 0$.

We generalize the result above to s-cycles of elliptic curves. In particular, an s-cycle is a collection of s primes $q_1, \ldots, q_s$ and s elliptic curves $E_1/\mathbb{F}_{q_1}, \ldots, E_s/\mathbb{F}_{q_s}$, such that $\cancel{|E_i(\mathbb{F}_{q_i})| = q_{i+1 \bmod s}}$ $\#E_i(\mathbb{F}_{q_i}) = q_{i+1 \bmod s}$. Among these, we are interested in ~~estimating the probability of finding cycles~~ finding those with small embedding degrees. As s increases, the number of cycles also increases. However, since the embedding degree condition is imposed on every step of the cycle, the probability decreases dramatically with s, as this is a very strong requirement.

~~In order to get a cycle we need an s-tuple of primes $q_1, \ldots, q_s$ that fit in the Hasse interval of each other, i.e. $|q_{i+1} - q_i - 1| \leq 2\sqrt{q_i}$. Throughout this section, all the constants in the proofs will be denoted c, although we remark that they might be different on each inequality or step of the proof~~We start by stating the main result of this section.

Theorem 5.2. *Let $s \geq 2$ ~~and $X \in \mathbb{Z}$~~, $K > 0$, and $M \in \mathbb{Z}$. Let $\mathfrak{p}$ be the probability of finding an s-cycle of elliptic curves ~~$(E_{q_1}, \ldots, E_{q_s})$ with $q_i \in [X, 2X]$~~ $E_1/\mathbb{F}_{q_1}, \ldots, E_s/\mathbb{F}_{q_s}$ with $q_i \in [M, 2M]$ and embedding degrees $k_i \leq K$ for all $i = 1, \ldots, s$, by sampling uniformly from all the s-cycles of elliptic curves with orders in the interval ~~$[X, 2X]$. Then~~ $[M, 2M]$. Then*

$$\mathfrak{p} < cK(K+1)\cancel{\frac{(\log\log X)^{2s}(\log X)^{3s}}{X^{s/2}}}\frac{(\log M)^{3s}(\log\log M)^{2s}}{M^{s/2}},$$

for some constant ~~c~~ $c > 0$ depending on s.

We will prove our result above through a sequence of lemmas. The overall strategy is as follows: in Lemma 5.3, we count the number of s-tuples of primes within the interval $[M, 2M]$ that are compatible with the Hasse condition. In Lemma 5.5, we impose an upper bound K on the embedding degree. Finally, in Lemmas 5.7 and 5.8, we count the curves that are compatible with the primes counted in the previous two results.

We start by disregarding the curves and just looking at the primes. In order to get a cycle, we need an s-tuple of primes $q_1, \ldots, q_s$ that fit in the Hasse interval of each other, i.e. $|q_{i+1} - q_i - 1| \leq 2\sqrt{q_i}$. Thus, we first count the s-tuples of possible primes $q_1, \ldots, q_s$ that are not too far apart.

Lemma 5.3. *Let $s \geq 2$ ~~a positive integer fixed~~ be a fixed positive integer and $C > 0$ a constant depending on s. For any ~~$X \geq 2$ we denote $T_s(X)$~~ $M \geq 2$ we denote by $T_s(M)$*

[3] In [4], the authors define pairing friendliness as having an embedding degree $k \leq (\log q)^2$. We will keep the bound as an unspecified parameter K.

the number of s-tuples of primes in the interval ~~$[X,2X]$ *with* $|q_i-q_j|\le C\sqrt{X}$~~ $[M,2M]$ *with* $|q_i-q_j|\le C\sqrt{M}$. *Then, there exist constants c_1, c_2 depending on s, such that*

$$c_1 \cancel{\frac{X^{(s+1)/2}}{(\log X)^s}} \frac{M^{(s+1)/2}}{(\log M)^s} \le T_s(\cancel{X}M) \le c_2 \cancel{\frac{X^{(s+1)/2}}{(\log X)^s}} \frac{M^{(s+1)/2}}{(\log M)^s}.$$

Proof. We split the interval ~~$[X,2X]$ in subintervals $I_k=[X+(k-1)C\sqrt{X}, X+kC\sqrt{X})$ for $1\le k\le \sqrt{X}/C$~~ $[M,2M]$ in subintervals $I_k=[M+(k-1)C\sqrt{M}, M+kC\sqrt{M})$ for $1\le k\le \lfloor\sqrt{M}/C\rfloor$ and call π_k the number of primes on the interval I_k. We denote ~~$X_C = X + C\left\lfloor\frac{\sqrt{X}}{C}\right\rfloor\sqrt{X}$~~ $M_C = M +$ Observe that ~~$2X - X_C \le C\sqrt{X}$~~ $2M - M_C \le C\sqrt{M}$ and, hence, the prime number theorem gives

$$\sum_{k=1}^{\cancel{\sqrt{X}/C}\,\lfloor\sqrt{M}/C\rfloor}\pi_k = \pi(\cancel{X}M_C)-\pi(\cancel{X}M) = \cancel{\frac{X}{\log X}}\frac{M}{\log M} + \cancel{E}e,$$

where ~~$|E|<\varepsilon\frac{X}{\log X}$~~ $|e|<\varepsilon\frac{M}{\log M}$ for any $\varepsilon>0$ and ~~$X>X_\varepsilon$~~ $M>M_\varepsilon$ sufficiently large, depending on ε. Then, a simple application of Hölder's inequality [7, Chapter 1, Theorem 2] for ~~$p=s, q=\frac{s}{s-1}$ gives us for $X>X_\varepsilon$~~

$$\cancel{(1-\varepsilon)\frac{X}{\log X} \le \sum_{k=1}^{\sqrt{X}/C}\pi_k \le \left(\sum_{k=1}^{\sqrt{X}/C}1\right)^{(s-1)/s}\left(\sum_{k=1}^{\sqrt{X}/C}\pi_k^s\right)^{1/s} \le cX^{(s-1)/2s}\left(\sum_{k=1}^{\sqrt{X}/C}\pi_k^s\right)^{1/s}}$$

$p=s$ and $q=\frac{s}{s-1}$ gives us that, for $M>M_\varepsilon$,

$$(1-\varepsilon)\frac{M}{\log M} \le \sum_{k=1}^{\lfloor\sqrt{M}/C\rfloor}\pi_k \le \left(\sum_{k=1}^{\lfloor\sqrt{M}/C\rfloor}1\right)^{(s-1)/s}\left(\sum_{k=1}^{\lfloor\sqrt{M}/C\rfloor}\pi_k^s\right)^{1/s}$$

$$\le c_1 M^{(s-1)/2s}\left(\sum_{k=1}^{\lfloor\sqrt{M}/C\rfloor}\pi_k^s\right)^{1/s}.$$

~~and hence~~ Hence,

$$\cancel{\frac{cX^{(s+1)/2}}{(\log X)^s}}\frac{c_2M^{(s+1)/2}}{(\log M)^s} \le \sum_{k=1}^{\cancel{\sqrt{X}/C}\,\lfloor\sqrt{M}/C\rfloor}\pi_k^s.$$

Finally, observe that every s-tuple of primes on each interval I_k is counted in ~~$T_s(X)$~~ $T_s(M)$, so we ~~will~~ can use the above expression to get a lower bound on ~~$T_s(X)$~~ $T_s(M)$. Let A be the set of indices k such that the interval I_k has more than $(s+1)^2$ primes. ~~Then, by the well known~~ Now, since for any $N_1>0$ and $N_2>1$ we have the following inequality [38, Corollary 2],

$$\pi(\cancel{M}N_1+N_2)-\pi(\cancel{M}N_1) \le \cancel{\frac{2M}{\log M}}\frac{2N_2}{\log N_2}, \tag{1}$$

we get ~~$\pi_k \le c\frac{\sqrt{X}}{\log X}$~~ that $\pi_k \le c_3\frac{\sqrt{M}}{\log M}$ for any k~~and hence~~. Therefore,

$$
\begin{aligned}
\frac{X}{\log X}\frac{M}{\log M} \sim \sum_{k\in A}\pi_k + \sum_{k\in\overline{A}}\pi_k &< c\frac{\sqrt{X}}{\log X}{}_3\frac{\sqrt{M}}{\log M}\#A| + (s+1)^2(\sqrt{X}\sqrt{M} - |\#A|) \\
&< c\frac{\sqrt{X}}{\log X}{}_3\frac{\sqrt{M}}{\log M}\#A| + (s+1)^2\sqrt{X}\sqrt{M},
\end{aligned}
$$

which gives us the bound

$$|\#A| > c\sqrt{X}_4\sqrt{M}$$

for any ~~X~~ M sufficiently large. Hence, ordering the primes to avoid repetitions, we get that

$$
\begin{aligned}
T_s(XM) &\ge \sum_{k=1}^{\sqrt{X}/C\lfloor\sqrt{M}/C\rfloor}\binom{\pi_k}{s} \ge \sum_{k\in A}\binom{\pi_k}{s} = \frac{1}{s!}\sum_{k\in A}\pi_k^s\prod_{j=0}^{s-1}\left(1-\frac{j}{\pi_k}\right) \\
&> \frac{1}{s!}\sum_{k\in A}\pi_k^s e^{-s(s+1)/\pi_k} > \frac{1}{s!e}\sum_{k\in A}\pi_k^s \\
&= \frac{1}{s!e}\left(\sum_{k=1}^{\sqrt{X}/C\lfloor\sqrt{M}/C\rfloor}\pi_k^s - \sum_{k\in\overline{A}}\pi_k^s\right) \ge c\frac{X^{(s+1)/2}}{(\log X)^s}{}_5\frac{M^{(s+1)/2}}{(\log M)^s} - \frac{1}{s!e}(s+1)^{2s}\sqrt{X}\sqrt{M} \\
&> c\frac{X^{(s+1)/2}}{(\log X)^s}{}_5\frac{M^{(s+1)/2}}{(\log M)^s}.
\end{aligned}
$$

In order to prove the second inequality, we denote the primes in the interval ~~$[X, 2X]$~~ $[M, 2M]$, in increasing order, as $q_1, \dots, q_N$. If we have an s-tuple starting with q_i, then the rest of the $s-1$ primes on the s-tuple will be in the interval ~~$I_i = (q_i, q_i + C\sqrt{X}]$~~ $I_i = (q_i, q_i + C\sqrt{M}]$. Hence, letting $\pi_i = \sum_{q\in I_i} 1$, we can apply the inequality ~~(1) to obtain~~ of Equation (1) to obtain

$$T_s(XM) \le \sum_{i=1}^{N}\binom{\pi_i}{s-1} \le c_6\sum_{i=1}^{N}\pi_i^{s-1} \le c\frac{X^{\frac{s-1}{2}}}{(\log X)^{s-1}}{}_7\frac{M^{\frac{s-1}{2}}}{(\log M)^{s-1}}N \le c\frac{X^{\frac{s+1}{2}}}{(\log X)^s}{}_8\frac{M^{\frac{s+1}{2}}}{(\log M)^s}. \tag{2}$$

□

Remark 5.4. For $s = 2$ and $C = 1$ we can get any constant $c_1 < 1/2$, by noting that

$$T_2(XM) \ge \frac{1}{2}\sum_{k=1}^{\sqrt{X}\sqrt{M}}\pi_k(\pi_k - 1) = \frac{1}{2}\sum_{k=1}^{\sqrt{X}\sqrt{M}}\pi_k^2 - \frac{1}{2}\sum_{k=1}^{\sqrt{X}\sqrt{M}}\pi_k \ge \frac{1}{2}\frac{X^{3/2}}{(\log X)^2}\frac{M^{3/2}}{(\log M)^2} - \frac{1}{2}\frac{X}{\log X}\frac{M}{\log M} \ge \Big(\frac{1}{2}$$

A different proof of the lower bound for the case $s = 2$ and $C = 1$, with a slightly ~~worst~~ worse constant, is given in [32, Lemma 1].

Now, let us impose the condition of having very small embedding degree.

Lemma 5.5. *For any* ~~$X>0$~~ $M>0$ *and* $K>0$, *let* ~~$T_{s,K}(X)$~~ $T_{s,K}(M)$ *be the number of* s*-tuples of primes in the interval* ~~$[X,2X]$, *with* $|q_i-q_j|\le C\sqrt{X}$~~ $[M,2M]$, *with* $|q_i-q_j|\le C\sqrt{M}$, *for some constant* $C>0$ *and such that* ~~$q_{i+1}|q_i^{k_i}-1$~~ $q_{i+1}\mid q_i^{k_i}-1$ *for some* $k_i\le K$. *Then*

$$T_{s,K}(\cancel{X}M)\le cK(K+1)\cancel{\sqrt{X}}\sqrt{M},$$

for some constant $c>0$.

Proof. We proceed similarly to [4]. First note that if ~~$q_{i+1}|q_i^{k_i}-1$, then $q_{i+1}|(q_i-q_{i+1})^{k_i}-1$~~ $q_{i+1}\mid q_i^{k_i}-1$, then $q_{i+1}\mid(q_i-q_{i+1})^{k_i}-1$ and, since ~~$|q_i-q_j|\le C\sqrt{X}$~~ $|q_i-q_j|\le C\sqrt{M}$, we have that for any i there exists an integer ~~$|h_i|\le C\sqrt{X}$ such that $q_{i+1}|h_i^{k_i}-1$~~ $|h_i|\le C\sqrt{M}$ such that $q_{i+1}\mid h_i^{k_i}-1$ for some $k_i\le K$. Now, since ~~$q_{i+1}>X\ge(Ch_i)^2$~~ $q_{i+1}>M\ge(Ch_i)^2$, we see that ~~$h^{k_i}-1$~~ $h_i^{k_i}-1$ has at most $c\frac{k_i}{2}$ prime divisors on the interval ~~$[X,2X]$~~ $[M,2M]$, for some constant $c>0$. Summing over the possible k and h we get

$$T_{s,K}(\cancel{X}M)\le\sum_{k\le K}\sum_{\cancel{|h|\le C\sqrt{X}}\,|h|\le C\sqrt{M}}\sum_{\cancel{q|h^k-1}\,q|h^k-1}1\le cK(K+1)\cancel{\sqrt{X}}\sqrt{M}.$$

□

Finally, we bring curves back into the equation. Given an interval $[M,2M]$, we will count the tuples of curves with orders in the intervals, and the subset of those such that every curve in the tuple is pairing-friendly. Theorem 5.2 will follow directly from these. We introduce the following result from [33], which we will require for the proof.

Lemma 5.6 ([33], Propositon 1.9). *Let* $q>3$ *be a prime number, let* $P\subset\mathbb{N}$ *and let* $N_{q,P}$ *be the number of isomorphism classes of elliptic curves over* $\mathbb{F}_q$ *and order* $\#E(\mathbb{F}_q)\in P$. *Then:*

– *If* $P\subseteq[q+1-2\sqrt{q},q+1+2\sqrt{q}]$, *then* $N_{q,P}\le c\#P(\log q)(\log\log q)^2\sqrt{q}$ *for some constant* $c>0$.

– *If* $P\subseteq[q-\sqrt{q},q+\sqrt{q}]$ *and* $\#P\ge 3$, *then* $N_{q,P}\ge c(\#P-2)\frac{\sqrt{q}}{\log q}$ *for some constant* $c>0$.

Lemma 5.7. *Let* ~~$C_s(X)$ *the set*~~ $M\ge 2$, *and let* $C_s(M)$ *be the number of* s*-tuples of elliptic curves* $E_1/\mathbb{F}_{q_1},\dots,E_s/\mathbb{F}_{q_s}$ *forming a cycle of length* s, ~~*and* $C_{s,K}(X)\subseteq C_s(X)$ *the subset in which* E_i *has embedding* $k_i\le K$~~ *where* $q_i\in[M,2M]$ *for all* $i=1,\dots,s$. *Then*

$$\cancel{c_1K\frac{X^{(2s+1)/2}}{(\log X)^{2s}}\le|C_s(X)|\le c_2K(\log\log X)^{2s}X^{(2s+1)/2}}$$
$$\cancel{|C_{s,k}(X)|\le c_3K(K+1)(\log X)^s(\log\log X)^{2s}X^{(s+1)/2}}$$

~~*for some constants* c_1,c_2,c_3~~ *there exist constants* c_1,c_2, *depending on* s~~.~~, *such that*

$$c_1\frac{M^{(2s+1)/2}}{(\log M)^{2s}}\le C_s(M)\le c_2(\log\log M)^{2s}M^{(2s+1)/2}.$$

Proof. First note that, if we have an s-cycle of curves, then the corresponding primes are as in Lemma 5.3 for any $C > s$. Without loss of generality, let us assume that cycles start at the smallest prime. Now, if we have an s-tuple in which the smallest prime is ~~p_i~~ q_i, then the rest of the $s-1$ primes on the s-tuple will be in the interval $I_i = (q_i, q_i + s\sqrt{q}_i + (s/2)^2]$. We can see this by induction. Let q_α, q_β be the ℓ-th and $(\ell+1)$-th primes in the cycle, respectively. The induction hypothesis is that $q_\alpha \leq q_i + 2\ell\sqrt{q}_i + \ell^2$. Then

$$\cancel{q_\beta \leq q_\alpha + 2\sqrt{q}_\alpha + 1 \leq q_i + 2\ell\sqrt{q}_i + \ell^2 + 2\sqrt{q_i + 2\ell\sqrt{q}_i + \ell^2} + 1 = q_i + 2(\ell+1)\sqrt{q}_i + (\ell+1)^2}$$

,

$$\begin{aligned} q_\beta &\leq q_\alpha + 2\sqrt{q}_\alpha + 1 \leq q_i + 2\ell\sqrt{q}_i + \ell^2 + 2\sqrt{q_i + 2\ell\sqrt{q}_i + \ell^2} + 1 \\ &= q_i + 2(\ell+1)\sqrt{q}_i + (\ell+1)^2. \end{aligned}$$

~~and then observe thatthe largest prime in the cyclecan only be~~ From here we deduce that, for any $l = 1, \ldots, s$, we have that

$$\sqrt{q_{l+i}} - \sqrt{q_i} \leq \ell.$$

Since they form a cycle, then it must be the case that $q_l \in I_i$ for all l. Note that there are at most $s/2$ ~~steps apart from the first one, since they form~~ primes between the largest and the smallest prime of a cycle.

Now, let us start by proving the upper bound for ~~$C_s(X)$. We know by [33, Proposition 1.9] that for every q and every subset of integers L such that for any $\ell \in L$, $|\ell - q + 1| \leq 2\sqrt{q}$,~~ $C_s(M)$. Let P be a subset of primes p satisfying that $|p - (q+1)| \leq 2q$. By the first part of Lemma 5.6, we know that there are at most ~~$c \log q (\log\log q)^2 \sqrt{q}|L|$~~ $c_1\sqrt{q}\log q(\log\log q)^2 \#P$ isomorphism classes over $\mathbb{F}_q$ of elliptic curves with ~~$|E(\mathbb{F}_q)| \in L$~~ $\#E(\mathbb{F}_q) \in P$ for some constant ~~c, so~~ c_1. Taking P with $\#P = s$ and multiplying over each prime of an s-tuple we get that, on each s-tuple, there will be less than

$$c_2(\log \cancel{X} M)^s(\log\log \cancel{X} M)^{2s} \cancel{X} M^{s/2}$$

isomorphism classes of elliptic curves with points on the s-tuple and, in particular, forming a cycle of length at most s. Note that the constant c_2 depends on s. Applying the second inequality of Lemma 5.3, we get the expected upper bound for cycles of length at most s, and in particular for ~~$C_s(X)$.~~ $C_s(M)$.

~~Now, to~~ To prove the lower bound for ~~$C_s(X)$ we see that the same Proposition 1.9 of [33] shows that for every subset of integers $L \in [q - \sqrt{q}, q + \sqrt{q}]$ with $|L| \geq 3$~~ $C_s(M)$ we will use the second part of Lemma 5.6. In this case, for any q and any subset of primes $P \subseteq [q - \sqrt{q}, q + \sqrt{q}]$ with $\#P \geq 3$ there are more than ~~$c(|L| - 2)\frac{\sqrt{q}}{\log q}$~~ $c_3(\#P - 2)\frac{\sqrt{q}}{\log q}$ isomorphism classes over $\mathbb{F}_q$ of elliptic curves with ~~$|E(\mathbb{F}_q)| \in S$~~ $\#E(\mathbb{F}_q) \in P$ for some constant ~~c, so~~ c_3. Hence, on each s-tuple with $s \geq 3$ we have more than ~~$c^s\frac{X^{s/2}}{(\log X)^s}$~~ $c_4\frac{M^{s/2}}{(\log M)^s}$ isomorphism classes of elliptic curves with points on the s-tuple and, in particular, forming a cycle of length at most s. Note that c_4 is a constant that depends on s. Observe that, in particular, all those primes lie on the Hasse interval for q, since $P \subset [q-\sqrt{q}, q+\sqrt{q}] \subset [q+1-2\sqrt{q}, q+1+2\sqrt{q}]$. Combining this with the first inequality of Lemma 5.3, we get the lower bound

$$c\frac{X^{(2s+1)/2}}{(\log X)^{2s}}5\frac{M^{(2s+1)/2}}{(\log M)^{2s}}.$$

~~Then, $C_s(X)$~~ Then, $C_s(M)$ will be cycles of isomorphism classes of elliptic curves of length at most s minus cycles of isomorphism classes of elliptic curves of length at most $s-1$~~, so~~. In order to bound the number of cycles of length at most $s-1$, we use the previous upper bound for $C_i(M)$, for $i = 1, \ldots, s-1$, so we get

$$C_s\sum_{i=1}^{s-1}(X\log\log M)c\frac{X^{(2s+1)/2}}{(\log X)^{2s}} - c\frac{X^{(2s-1)/2}}{(\log X)^{2s-2}}{}^{2i}M^{(2i+1)/2} \leq c\frac{X^{(2s+1)/2}}{(\log X)^{2s}}{,}_{6}(\log\log M)^{2s-2}M^{(2s-1)/2}$$

for ~~X~~ some constant c_6. Hence,

$$C_s(M) \geq c_5\frac{M^{(2s+1)/2}}{(\log M)^{2s}} - c_6(\log\log M)^{2s-2}M^{(2s-1)/2} \geq c_7\frac{M^{(2s+1)/2}}{(\log M)^{2s}},$$

for some constant c_7 and for M sufficiently large depending on s.

~~Finally, the proof of the upper bound for $C_{s,K}(X)$ is the same, now using Lemma5.5 instead.~~ □

~~As a corollary of the previous Lemma~~By mimicking the second part of the previous proof, but using Lemma 5.5 instead of Lemma 5.3, we obtain the following analogous result.

Lemma 5.8. *Let $M \geq 2$. Let $C_{s,K}(M)$ be the number of s-tuples in the same conditions as in Lemma 5.7, which additionally satisfy that E_i has embedding $k_i \leq K$ for all $i = 1, \ldots, s$. Then there exists a constant c, depending on s, such that*

$$C_{s,K}(M) \leq cK(K+1)(\log M)^s(\log\log M)^{2s}M^{(s+1)/2}.$$

Finally, from Lemmas 5.7 and 5.8, we get Theorem 5.2 ~~, by just dividing $C_{s,K}(X)$ by $C_s(X)$~~by dividing $C_{s,K}(M)$ by $C_s(M)$.

6 Conclusions

Cycles of elliptic curves require the curves involved to be of prime order, and families of elliptic curves parameterized by low-degree polynomials are the only known approach at generating pairing-friendly curves with prime order. In this work, we have shown that this approach is unlikely to yield new cycles, beyond the MNT4-MNT6 cycles that are already known. In particular, we have shown that no known families are involved in a 2-cycle with any pairing-friendly curve of cryptographic interest. Along the way, we have developed our understanding of these mathematical objects, showing some new properties and a probability analysis.

While a lot is still unknown about pairing-friendly cycles, we highlight two avenues that we consider interesting for future research.

– Generalizing Theorem 4.5 and Corollary 4.8 to s-cycles, for $s > 2$. The case $s = 2$ is the most appealing from a practical perspective, due to the application to recursive composition of SNARKs, but it would be desirable to have the complete picture. The main hurdle here is that, whereas fixing a curve in a 2-cycle automatically determines the other, longer cycles have more degrees of freedom, so we do not have as much explicit information to work with in the proof.
– Consider a 2-cycle such that both curves $E \leftrightarrow (t, p, q)$ and $E' \leftrightarrow (2 - t, q, p)$ have the same embedding degree k. If we restrict ourselves to the case $k \equiv 0 \pmod 4$, it is easy to argue (as in Proposition 3.10) that

$$pq \mid \Phi_k(t - 1).$$

This approach allows [14] to prove that said cycles cannot exist when $k \in \{8, 12\}$. However, the authors leave higher values of k as an open question. If we consider families of curves, Theorem 4.5 tells us that the above relation must hold as polynomials, or else only a finite number of cycles will exist. Thus, we wonder if considering the above condition as a relation between polynomials, and applying polynomial machinery, could help in answering this question.

References

1. SageMath code from Appendix C. GitHub repository (2022), `https://github.com/pairingfriendlycycles/pairing-friendly-cycles/tree/main` 4, 30
2. Aranha, D.F., Housni, Y.E., Guillevic, A.: A survey of elliptic curves for proof systems. Cryptology ePrint Archive, Paper 2022/586 (2022), `https://eprint.iacr.org/2022/586`, `https://eprint.iacr.org/2022/586`
3. Atkin, A.O.L., Morain, F.: Elliptic curves and primality proving. Mathematics of computation **61**(203), 29–68 (1993)
4. Balasubramanian, R., Koblitz, N.: The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm. J. Cryptology **11**(2), 141–145 (1998) 4, 18, 19, 22
5. Barreto, P.S., Lynn, B., Scott, M.: Constructing elliptic curves with prescribed embedding degrees. In: International conference on security in communication networks. pp. 257–267. Springer (2002) 5
6. Barreto, P.S., Naehrig, M.: Pairing-friendly elliptic curves of prime order. In: International workshop on selected areas in cryptography. pp. 319–331. Springer (2005) 3, 5, 7
7. Beckenbach, E.F., Bellman, R.: Inequalities (1961) 20
8. Ben-Sasson, E., Chiesa, A., Tromer, E., Virza, M.: Scalable zero knowledge via cycles of elliptic curves. Algorithmica **79**(4), 1102–1160 (2017) 1, 2, 3
9. Bitansky, N., Canetti, R., Chiesa, A., Tromer, E.: From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again. In: Proceedings of the 3rd Innovations in Theoretical Computer Science Conference. pp. 326–349 (2012) 1
10. Bonneau, J., Meckler, I., Rao, V., Shapiro, E.: Mina: Decentralized cryptocurrency at scale. New York Univ. O (1) Labs, New York, NY, USA, Whitepaper pp. 1–47 (2020) 1
11. Bowe, S., Grigg, J., Hopwood, D.: Recursive proof composition without a trusted setup. Cryptology ePrint Archive (2019) 2
12. Bünz, B., Chiesa, A., Mishra, P., Spooner, N.: Proof-carrying data from accumulation schemes. Cryptology ePrint Archive (2020) 2
13. Cahen, P.J., Chabert, J.L.: What you should know about integer-valued polynomials. The American Mathematical Monthly **123**(4), 311–337 (2016) 31

14. Chiesa, A., Chua, L., Weidner, M.: On cycles of pairing-friendly elliptic curves. SIAM Journal on Applied Algebra and Geometry **3**(2), 175–192 (2019) 2, 3, 10, 13, 18, 25
15. Chiesa, A., Tromer, E.: Proof-carrying data and hearsay arguments from signature cards. In: ICS. vol. 10, pp. 310–331 (2010) 1
16. Chiesa, A., Tromer, E., Virza, M.: Cluster computing in zero knowledge. In: Advances in Cryptology-EUROCRYPT 2015: 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part II 34. pp. 371–403. Springer (2015) 1
17. Costello, C., Fournet, C., Howell, J., Kohlweiss, M., Kreuter, B., Naehrig, M., Parno, B., Zahur, S.: Geppetto: Versatile verifiable computation. In: 2015 IEEE Symposium on Security and Privacy. pp. 253–270 (2015). https://doi.org/10.1109/SP.2015.23 2
18. Cox, D.A.: Primes of the form x^2+ny^2: Fermat, class field theory, and complex multiplication. John Wiley & Sons (1989) 4
19. Crandall, R., Pomerance, C.: Prime numbers: A computational perspective. Springer-Verlag, New York (2001)
20. El Housni, Y., Guillevic, A.: Families of SNARK-friendly 2-chains of elliptic curves. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 367–396. Springer (2022) 3
21. Freeman, D.: Constructing pairing-friendly elliptic curves with embedding degree 10. In: International Algorithmic Number Theory Symposium. pp. 452–465. Springer (2006) 3, 5, 7
22. Freeman, D.: Constructing pairing-friendly elliptic curves with embedding degree 10 (2006), `https://theory.stanford.edu/~dfreeman/talks/ants.pdf`, presentation slides from ANTS-VII 8
23. Freeman, D., Scott, M., Teske, E.: A taxonomy of pairing-friendly elliptic curves. Journal of cryptology **23**(2), 224–280 (2010) 5
24. Frey, G., Rück, H.G.: A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. Mathematics of computation **62**(206), 865–874 (1994) 5
25. Gabizon, A., Williamson, Z.J., Ciobotaru, O.: PlonK: Permutations over Lagrange-bases for oecumenical noninteractive arguments of knowledge. Cryptology ePrint Archive (2019) 1
26. Galbraith, S.D., McKee, J.F., Valença, P.C.: Ordinary abelian varieties having small embedding degree. Finite Fields and Their Applications **13**(4), 800–814 (2007) 3, 7
27. Groth, J.: On the size of pairing-based non-interactive arguments. In: Fischlin, M., Coron, J. (eds.) Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part II. Lecture Notes in Computer Science, vol. 9666, pp. 305–326. Springer (2016) 1
28. Hardy, G.H., Wright, E.M.: An Introduction to the Theory of Numbers. Oxford University Press, Great Clarendon Street, Oxford OX2 6DP, sixth edn. (1975)
29. Karabina, K., Teske, E.: On prime-order elliptic curves with embedding degrees $k = 3, 4$, and 6. In: International Algorithmic Number Theory Symposium. pp. 102–117. Springer (2008) 3
30. Kate, A., Zaverucha, G.M., Goldberg, I.: Constant-size commitments to polynomials and their applications. In: International conference on the theory and application of cryptology and information security. pp. 177–194. Springer (2010)
31. Kattis, A., Bonneau, J.: Proof of necessary work: Succinct state verification with fairness guarantees. Cryptology ePrint Archive (2020) 1
32. Koblitz, N.: Elliptic curve implementation of zero-knowledge blobs. J. Cryptology **4**(3), 207–213 (1991) 21
33. Lenstra, Jr., H.W.: Factoring integers with elliptic curves. Ann. of Math. (2) **126**(3), 649–673 (1987) 22, 23
34. Matthews, K.: The diophantine equation $x^2 - dy^2 = n, d > 0$. Expositiones Mathematicae **18**(4), 323–332 (2000)

35. Menezes, A.J., Okamoto, T., Vanstone, S.A.: Reducing elliptic curve logarithms to logarithms in a finite field. iEEE Transactions on information Theory **39**(5), 1639–1646 (1993) 3, 5
36. Migotti, A.: Zur Theorie der Kreisteilungsgleichung. B. der Math.-Naturwiss, Classe der Kaiserlichen Akademie der Wissenschaften, Wien **87**, 7–14 (1883) 11
37. Miyaji, A., Nakabayashi, M., Takano, S.: New explicit conditions of elliptic curve traces for FR-reduction. IEICE transactions on fundamentals of electronics, communications and computer sciences **84**(5), 1234–1243 (2001) 3, 5, 7
38. Montgomery, H.L., Vaughan, R.C.: The large sieve. Mathematika **20**(2), 119–134 (1973) 20
39. Naveh, A., Tromer, E.: PhotoProof: Cryptographic image authentication for any set of permissible transformations. In: 2016 IEEE Symposium on Security and Privacy (SP). pp. 255–271. IEEE (2016) 1
40. Parno, B., Howell, J., Gentry, C., Raykova, M.: Pinocchio: Nearly practical verifiable computation. vol. 59, pp. 238–252 (05 2013). https://doi.org/10.1109/SP.2013.47 1
41. Pegg, E.J.: Bouniakowsky conjecture. MathWorld–A Wolfram Web Resource, created by Eric W. Weisstein `https://mathworld.wolfram.com/BouniakowskyConjecture.html` 6
42. Pohlig, S., Hellman, M.: An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance (corresp.). IEEE Transactions on information Theory **24**(1), 106–110 (1978)
43. Silverman, J.H.: The arithmetic of elliptic curves, vol. 106. Springer (2009) 4, 7
44. Silverman, J.H., Stange, K.E.: Amicable pairs and aliquot cycles for elliptic curves. Experimental Mathematics **20**(3), 329–357 (2011) 2, 9, 10
45. Smart, N.P.: The discrete logarithm problem on elliptic curves of trace one. JOURNAL OF CRYPTOLOGY **12**, 193–196 (1999) 2
46. Sutherland, A.V.: Accelerating the CM method. LMS Journal of Computation and Mathematics **15**, 172–204 (2012) 5
47. Valiant, P.: Incrementally verifiable computation or proofs of knowledge imply time/space efficiency. In: Theory of Cryptography Conference. pp. 1–18. Springer (2008) 1
48. Weisstein, E.W.: Cyclotomic polynomial. MathWorld–A Wolfram Web Resource `https://mathworld.wolfram.com/CyclotomicPolynomial.html`

A Polynomial division

In this section, we show that $p(X)^\ell \bmod q(X)$ is an integer-valued polynomials, when $E \leftrightarrow (t,p,q)$ are either the MNT3 or BN curves. This is completely analogous to the argument in Remark 4.6.

MNT3 curves. In this case, $q(X) = 12X^2 - 1$. We proceed by induction on ℓ. For $\ell = 1$, we have that

$$p(X) \bmod q(X) = -6X + 2,$$

which is of the form $6aX + b$, for some $a, b \in \mathbb{Z}$. We show that, if $p^\ell \bmod q$ is of this form, then so is $p^{\ell+1} \bmod q$. Then all the remainders will actually be in $\mathbb{Z}[X]$.

Assume that there exist $a, b, c, d \in \mathbb{N}$ such that

$$p(X)^\ell \bmod q(X) = 6aX + b.$$

Then

$$\begin{aligned} p(X)^{\ell+1} &\equiv p(X)^\ell p(X) \equiv (6aX + b)(-6X + 2) \\ &\equiv -36aX^2 + (12a - 6b)X + 2b \\ &\equiv (-12a + 6b)X + (-3a + 2b) \pmod{q(X)}. \end{aligned}$$

Since the coefficient of degree 1 is divisible by 6, the induction step works.

BN curves. In this case, $q(X) = 36X^4 + 36X^3 + 24X^2 + 6X + 1$. Assume that there exist $a, b, c, d \in \mathbb{N}$ such that

$$p(X)^\ell \bmod q(X) = 36aX^3 + 6bX^2 + 6cX + d,$$

for some $a, b, c, d \in \mathbb{Z}$. Then

$$\begin{aligned} p(X)^{\ell+1} &\equiv p(X)^\ell p(X) \equiv \left(36aX^3 + 6bX^2 + 6cX + d\right)\left(-6X^2\right) \\ &\equiv -216aX^5 - 36bX^4 - -36cX^3 - 6dX^2 \\ &\equiv (-72a + 36b - 36c)X^3 + (-108a + 24b - 6d)X^2 \\ &\quad +(-30a + 6b)X + (-6a + b) \pmod{q(X)}. \end{aligned}$$

Since the coefficient of degree 3 is divisible by 36, and the coefficients of degree 2 and 1 are divisible by 6, the induction step works.

B Tables

Bounds for MNT3

ℓ	$\cancel{A}\, N_{\mathrm{left}}$	$\cancel{B}\, N_{\mathrm{right}}$
5	-104	104
10	-75658	75657
19	-10626317415	10626317415

Bounds for Freeman

ℓ	$\cancel{A}\, N_{\mathrm{left}}$	$\cancel{B}\, N_{\mathrm{right}}$
3	-2	4
6	-164	161
7	-686	685
9	-10608	10607
13	-1805067	1805066
14	-6158596	6158595
17	-210958904	210958905
18	-643610018	643610019
19	-1875810507	1875810508
21	-12522961240	12522961243
23	-15125575810	15125575853

Bounds for BN

ℓ	$\cancel{A}\, N_{\mathrm{left}}$	$\cancel{B}\, N_{\mathrm{right}}$
3	-1	0
4	-3	4
5	-12	11
6	-15	4
7	-65	64
8	-104	103
9	-167	168
10	-831	830
11	-513	508
12	-3523	3524
13	-8620	8619
14	-4092	4097
15	-52351	52350
16	-66417	66414
17	-164463	164464
18	-626817	626816
19	-186373	186364
20	-2992820	2992819
21	-6014684	6014683
22	-5673471	5673474
23	-41263041	41263040
24	-39448697	39448694
25	-151319223	151319224
26	-462478015	462478014
27	-20593636	20593693
28	-2473968276	2473968275
29	-4050737756	4050737755
30	-6238668798	6238668799
31	-31854421247	31854421246
32	-20649322466	20649322461

Table 3. Bounds ~~A, B~~ $N_{\mathrm{left}}, N_{\mathrm{right}}$ from Lemma 4.4 for different embedding degrees ℓ of the potential partner curve of MNT3, Freeman, and BN curves. The remaining values of $\ell \leq 20$ are covered by Corollaries 4.2 and 4.3 for MNT3 and Freeman curves, respectively.

C ~~SageMath code~~

Supplementary material - SageMath code

This code is available at [1].

B.1 Setup

`MNT3(), MNT4(), MNT6(), Freeman(), BN()`

These functions return the set of polynomials that define the families of curves MNT3, MNT4, MNT6, Freeman, and BN, respectively.

The expected outputs are:

- t: polynomial $t(X) \in \mathbb{Q}[X]$ that parameterizes the trace.
- p: polynomial $p(X) \in \mathbb{Q}[X]$ that parameterizes the order of the curves.
- q: polynomial $q(X) \in \mathbb{Q}[X]$ that parameterizes the order of the finite field over which the curve is defined.

```
# SETUP

# Polynomial rings over the reals and rationals.
R.<X> = PolynomialRing(RR, 'X')
Q.<X> = PolynomialRing(QQ, 'X')

# Curve families.
def MNT3():
    t = Q(6*X -1)
    q = Q(12*X^2 - 1)
    p = q + 1 - t
    return(t, p, q)

def MNT4():
    t = Q(-X)
    q = Q(X^2 + X + 1)
    p = q + 1 - t
    return(t, p, q)

def MNT6():
    t = Q(2*X + 1)
    q = Q(4*X^2 + 1)
    p = q + 1 - t
    return(t, p, q)

def Freeman():
    t = Q(10*X^2 + 5*X + 3)
    q = Q(25*X^4 + 25*X^3 + 25*X^2 + 10*X + 3)
    p = q + 1 - t
    return(t, p, q)

def BN():
    t = Q(6*X^2 + 1)
    q = Q(36*X^4 + 36*X^3 + 24*X^2 + 6*X + 1)
    p = q + 1 - t
    return(t, p, q)
```

B.2 Code for Proposition 4.1

`candidate_embedding_degrees(Family, K_low, K_high)`

Given a family of curves, this function computes the possible embedding degrees of curves that may form 2-cycles with a curve of the given family.

The expected inputs are:

- Family: a polynomial parameterization $(t(X), p(X), q(X))$ of a family of pairing-friendly elliptic curves with prime order.
- K_low, K_high: lower and upper bounds on the embedding degree to look for.

The expected outputs are:

- embedding_degrees: a list of potential embedding degrees k such that K_low $\leq k \leq$ K_high and a curve from the family *might* form a cycle with a curve with embedding degree k.
- modular_conditions: conditions on x mod k for each of these k.

```
def candidate_embedding_degrees(Family, K_low, K_high):

    (t, p, q) = Family()
    # Create an empty list to store the candidate embedding degrees
    embedding_degrees = []
    # Create an empty list to store the lists of modular conditions for each k
    modular_conditions = [None] * (K_high + 1)

    # Embedding degree k implies that q(x) = 1 (mod k).
    # We check this condition in 0, ..., k-1 and build a list of candidates
    # such that any x has to be congruent to one of them modulo k.
    for k in range(K_low, K_high + 1):

        candidate = False

        for i in range(k):
            if ((q(i) % k) == 1):
                # First time a candidate k is discovered, add it to the list and
                # create a list within modular_conditions to store the values i.
                if (not candidate):
                    candidate = True
                    embedding_degrees.append(k)
                    modular_conditions[k] = []
                modular_conditions[k].append(i)

    return embedding_degrees, modular_conditions
```

B.3 Auxiliary functions

is_integer_valued(g)

This function checks whether a given polynomial g is integer-valued. It returns True if so, and False otherwise. The test is based on the fact that a polynomial $g \in \mathbb{Q}[X]$ is integer-valued if and only if $g(x) \in \mathbb{Z}$ for $\deg g + 1$ consecutive $x \in \mathbb{Z}$ [13, Corollary 2].

```
def is_integer_valued(g):

    # Check if evaluation is integer in deg(g) + 1 consecutive points.
    for x in range(g.degree()+1):
        if (not g(x) in ZZ):
            print(str(g) + " is not integer-valued.")
            return False
    return True
```

`find_relevant_root(w, b, side)`

This function finds the left-most or right-most root of a polynomial $b(X) \in \mathbb{Q}[X]$.

The expected inputs are:

- `w`: positive integer.
- `b`: polynomial $b(X) \in \mathbb{Q}[X]$.
- `side`: this parameter specifies which root to keep. If `side = -1`, then the function takes the left-most root, and if `side` $= 1$, it returns the right-most root.

The expected output is the relevant extremal root.

```
def find_relevant_root(w, b, side):
    # Decide whether to keep the left-most or right-most root.
    i = -(1 + side) / 2
    # 0 <= w(x)
    C_1 = 0
    w_roots = R(w).roots()
    if (w_roots != []):
        C_1 = w_roots[i][0]
    # w(x) < b(x)
    C_2 = 0
    bw_roots = R(b - w).roots()
    if (bw_roots != []):
        C_2 = bw_roots[i][0]
    # Return the relevant extremal root.
    if (side == -1):
        return ceil(min(C_1, C_2))
    else:
        return floor(max(C_1, C_2))
```

`check_embedding_degree(px, qx, k)`

This function determines whether k is the smallest positive integer such that $(\texttt{px}^k - 1) \pmod{\texttt{qx}} = 1$, and outputs `True/False`.

```
def check_embedding_degree(px, qx, k):
    # Checks divisibility condition
    if ((px^k - 1) % qx != 0): return False
    # Checks that divisibility conditions does not happen for smaller
    exponents
    div = divisors(k)
    div.remove(k)
    for j in div:
        if ((px^j - 1) % qx == 0):
            return False
    return True
```

B.4 Code for Table 3

`compute_bounds(a, b)`

This function computes the bounds $N_{\mathsf{left}}, N_{\mathsf{right}}$ of Lemma 4.4. This function has been used to produce the results of tables from Figure 3. It uses the auxiliary functions from Appendix B.3.

The expected inputs are:

– `a, b`: two integer-valued polynomials in $\mathbb{Q}[X]$.

The expected outputs are:

– `N_left, N_right`: integer bounds $N_{\mathsf{left}}, N_{\mathsf{right}}$ described in Lemma 4.4.

```
def compute_bounds(a, b):

    # Check that b has even degree and positive leading coefficient
    if (b.degree() % 2 == 1 or b.leading_coefficient() < 0):
        print("Invalid divisor.")
        return

    # Check that a, b are integer valued.
    if (not is_integer_valued(a) or not is_integer_valued(b)):
        return

    # Polynomial division
    (h, r) = a.quo_rem(b)

    # Compute c so that ch, cr are in Z[X]
    denominators = [i.denominator() for i in (h.coefficients() + r.coefficients())]
    c = lcm(denominators)

    # Compute signs
    sigma_right = sign(r.leading_coefficient())
    sigma_left = sigma_right * (-1)^(r.degree())

    # We compute the polynomials w_left, w_right such that
    # 0 <= w_left < b(x) for all x < N_left, and
    # 0 <= w_right < b(x) for all x > N_right.
    w_left = c * r + ((1 - sigma_left) / 2) * b
    w_right = c * r + ((1 - sigma_right) / 2) * b

    # Compute N_left, N_right
    N_left = find_relevant_root(w_left, b, -1)
    N_right = find_relevant_root(w_right, b, 1)

    return (N_left, N_right)
```

B.5 Code for Corollary 4.8

`exhaustive_search(Family, k, N_left, N_right, mod_cond)`

This function performs the exhaustive search from Corollary 4.8 within the intervals $[N_{\mathsf{left}}, N_{\mathsf{right}}]$.

The expected inputs are:

– `Family`: a polynomial parameterization $(t(X), p(X), q(X))$ of a family of pairing-friendly elliptic curves with prime order.
– `k`: an embedding degree.
– `N_left, N_right`: upper and lower integer bounds.
– `mod_cond`: conditions on $x \bmod$ `k` for every x in the interval [`N_left, N_right`].

The expected output is:

- `curves`: a list of curve descriptions $(x, k, t(x), p(x), q(x))$ such that $x \in$ [`N_left, N_right`], and the curve parameterized by $(t(x), p(x), q(x))$ forms a cycle with a curve with embedding degree `k`.

```
def exhaustive_search(Family, k, N_left, N_right, mod_cond):

  (t, p, q) = Family()
  curves  = []

  for x in range(N_left, N_right+1):
      # We skip those values that will never yield q(x) = 1 (mod k), as
    precomputed above.
      if (not (x % k) in mod_cond): continue
      # Check the embedding degree condition
      if (check_embedding_degree(p(x), q(x), k)):
          curves.append((x, k, t(x), p(x), q(x)))

  return curves
```

B.6 Main function

`search_for_cycles(Family, K_low, K_high)`

This function looks for 2-cycles formed by a curve belonging to a given parameterized family of curves and a prime-order curve with an embedding degree between two given bounds.

The expected inputs are:

- `Family`: a polynomial parameterization $(t(X), p(X), q(X))$ of a family of pairing-friendly elliptic curves with prime order.
- `K_low, K_high`: integer lower and upper bounds on the embedding degree to look for.

The function prints to a file all 2-cycles involving a curve from the family and a prime-order curve with embedding degree `K_low` $\leq k \leq$ `K_high`.

```
import time

def search_for_cycles(Family, K_low, K_high):

    file_name = 'output_' + Family.__name__ + '.txt'
    f = open(file_name, 'w')
    start = time.time()

    # Instantiate the family
    (t, p, q) = Family()
    print("Starting family: " + str(Family.__name__), file=f)
    print("t(X) = " + str(t), file=f)
    print("p(X) = " + str(p), file=f)
    print("q(X) = " + str(q), file=f)

    # Find the candidate embedding degrees up to K that are compatible with this family
    (embedding_degrees, modular_conditions) = candidate_embedding_degrees(Family, K_low, K_high)
    print("Candidate embedding degrees: " + str(embedding_degrees), file=f)
    for k in embedding_degrees:
        print(("For k = " + str(k) + ", necessarily x = " +str(modular_conditions[k])) + " (mod " + str(k) + ")", file=f)
    print("=======================", file=f)

    # For each potential embedding degree, find the bounds N_left, N_right and perform exhaustive search within [N_left, N_right].
    for k in embedding_degrees:

        f.close()
        f = open(file_name, 'a')
        start_k = time.time()

        print("k = " + str(k), file=f)
        (N_left, N_right) = compute_bounds(p^k, q)
        print("N_left = " + str(N_left) + ", N_right = " + str(N_right), file=f)

        curves = exhaustive_search(Family, k, N_left, N_right, modular_conditions[k])
        print("Curves with embedding degree " + str(k) + " that form a cycle with a curve from the " + str(Family.__name__) + " family: " + str(len(curves)), file=f)

        for curve in curves:
            (x, k, tx, px, qx) = curve
            print("x = " + str(x), file=f)
            print("embedding degree = " + str(k), file=f)
            print("t(x) = " + str(tx), file=f)
            print("p(x) = " + str(px), file=f)
            print("q(x) = " + str(qx), file=f)
            print("------------", file=f)

        end_k = time.time()
        print('Computations for embedding degree ' + str(k) + ' took', round(end_k - start_k, 2), 'seconds.', file=f)
        print("------------------------", file=f)

    end = time.time()
    print("=======================", file=f)
    print('Overall computation took', round(end - start, 2), 'time', file=f)

    f.close()
```