SIAM J. APPL. ALGEBRA GEOMETRY
Vol. 3, No. 2, pp. 175–192

On Cycles of Pairing-Friendly Elliptic Curves*

Alessandro Chiesa†, Lynn Chua†, and Matthew Weidner‡

Abstract. A cycle of elliptic curves is a list of elliptic curves over finite fields such that the number of points on one curve is equal to the size of the field of definition of the next, in a cyclic way. We study cycles of elliptic curves in which every curve is pairing-friendly. These have recently found notable applications in pairing-based cryptography, for instance, in improving the scalability of distributed ledger technologies. We construct a new cycle of length 4 consisting of MNT curves, and characterize all the possibilities for cycles consisting of MNT curves. We rule out cycles of length 2 for particular choices of small embedding degrees. We show that long cycles cannot be constructed from families of curves with the same complex multiplication discriminant, and that cycles of composite order elliptic curves cannot exist. We show that there are no cycles consisting of curves from only the Freeman or Barreto–Naehrig families.

Key words. elliptic curves, Weil pairing, cryptography

AMS subject classifications. 14H52, 14G50, 11T71

DOI. 10.1137/18M1173708

1. Introduction.

A cycle of elliptic curves is a list of elliptic curves defined over finite fields in which the number of points on one curve equals the size of the field of definition of the next, cyclically.

Definition 1.1. *An* m-cycle of elliptic curves *is a list of* m *distinct elliptic curves* $E_1/\mathbb{F}_{q_1}$*,* $\ldots$*,* $E_m/\mathbb{F}_{q_m}$*, where* $q_1, \ldots, q_m$ *are prime, such that the numbers of points on these curves satisfy*

$$\#E_1(\mathbb{F}_{q_1}) = q_2\,, \ldots, \#E_i(\mathbb{F}_{q_i}) = q_{i+1}\,, \ldots, \#E_m(\mathbb{F}_{q_m}) = q_1\,. \tag{1.1}$$

This notion was introduced in [33] with the name of *aliquot cycles*. The case of 2-cycles of ordinary curves, also called *amicable pairs*, was introduced in the context of primality proving by [25, 26] under the equivalent notion of *dual elliptic primes* (see Appendix A).

Silverman and Stange [33] showed that cycles of arbitrary lengths exist, and gave conjectural estimates for any elliptic curve $E/\mathbb{Q}$ of the number of prime pairs (q_1, q_2) such that reducing E modulo q_1 and q_2 gives an amicable pair. Cycles of elliptic curves were further studied in [1, 20, 28, 29], and some of these works refined and proved on average the conjectured estimates, showing that amicable pairs are asymptotically common.

*Received by the editors March 5, 2018; accepted for publication (in revised form) January 29, 2019; published electronically April 2, 2019.
http://www.siam.org/journals/siaga/3-2/M117370.html
Funding: The first author was supported by the UC Berkeley Center for Long-Term Cybersecurity. The second author was supported by a UC Berkeley University Fellowship.
†Department of Electrical Engineering and Computer Science, UC Berkeley, Berkeley, CA 94720 (alexch@berkeley.edu, chualynn@berkeley.edu).
‡Computer Laboratory, University of Cambridge, Cambridge, CB3 0FD, UK (malw2@cam.ac.uk).

In [4] the notion of cycles of elliptic curves was extended for applications to pairing-based cryptography.

Definition 1.2. *A* pairing-friendly m-cycle of elliptic curves *is an m-cycle such that every elliptic curve in the cycle is ordinary and has a small embedding degree.*

Pairing-friendly cycles were used in [4] to achieve recursive composition of *zkSNARKs* (also known as *proof carrying data*). A zkSNARK is a cryptographic scheme that allows one party (the prover) to convince another party (the verifier) that the prover knows a certain secret, via a short proof that is cheap to verify and reveals no information about the secret. Efficient zkSNARK constructions are obtained via pairing-friendly elliptic curves, and the cycle condition in (1.1) enables their recursive composition, while avoiding expensive modular arithmetic across fields of different characteristics. (See [4] for details.)

Practitioners are interested in recursive composition of zkSNARKs, because it can be used to boost the scalability of distributed ledger technologies [10]. For example, there are commercial efforts in this space whose core technology *is* recursive composition [13], and such technology thus rests on properties of cycles of pairing-friendly elliptic curves.

This motivates the question: *What types of pairing-friendly cycles exist?*

A pairing-friendly 2-cycle can be obtained from pairing-friendly prime-order curves of embedding degrees 4 and 6 [22, 4]. Beyond this, there are *no* other known constructions, and very little is known about pairing-friendly cycles. Indeed, requiring a small embedding degree as in Definition 1.2 is a strong restriction and techniques used in previous work to study aliquot cycles do not seem to apply to pairing-friendly cycles.

This is unfortunate because the aforementioned MNT cycle is not ideal for applications: its unequal embedding degrees make one curve less secure than the other; moreover, the fact that both embedding degrees are so small implies that using the cycle at high security levels is inefficient. It would be desirable, e.g., to have a 2-cycle with embedding degrees $(12, 12)$ or $(20, 20)$ and, more generally, to understand this mathematical object better.

1.1. Overview of results. The stark difference in the current understanding of pairing-friendly cycles when compared to aliquot cycles, as well as applications to pairing-friendly cryptography in the real world, motivates a systematic study of pairing-friendly cycles. In this paper we initiate such a study with the following main results.

1. Prior to this work, the *only* construction of pairing-friendly cycles was a 2-cycle from a family of curves called *MNT curves*, named after Miyaji, Nakabayashi, and Takano [27]. A natural question to ask is: Can one construct other cycles consisting of MNT curves? In this work, we construct a new pairing-friendly cycle of length 4 using MNT curves. We also characterize *all* the possibilities for cycles consisting of MNT curves, showing that any MNT cycle must have length 2 or 4, and that the curves must have embedding degrees alternating between 4 and 6. See section 4 for details.
2. We then study *arbitrary* pairing-friendly 2-cycles (not derived from a particular family). We prove that 2-cycles of elliptic curves with embedding degrees $(5, 10)$, $(8, 8)$, or $(12, 12)$ do *not* exist. The technique that we use relies on the fact that the cyclotomic polynomials of these embedding degrees have degree 4. In particular, we do not know how to extend this result to any other embedding degrees (k_1, k_2). See section 5 for

details.

3. We move to study pairing-friendly cycles of arbitrary length. One strategy to construct cycles could be to pick a parametrized family of elliptic curves and try to construct cycles consisting of curves from the same family (like for MNT curves). What must the parameters of the family satisfy for such constructions to be possible? We prove that if the curves have the same discriminant for complex multiplication $D > 3$, then we cannot construct cycles of length greater than 2 (section 6). This implies that to construct elliptic curve cycles, we must use curves from families of varying discriminants.
4. So far we discussed cycles consisting of elliptic curves of *prime* order. What if we relax the definition of cycles to allow *composite* (nonprime) order elliptic curves in which the number of points on one curve is a multiple of (but not necessarily equal to) the size of the field of definition of the next? We prove that composite-order cycles *cannot exist* (see section 7). This is a strong restriction as it implies that we must construct cycles using pairing-friendly elliptic curves of *prime* order. Unfortunately, there are very few constructions of families of such curves in the literature, *regardless of cycles*.
5. Last, we study the other known families of pairing-friendly elliptic curves of prime order (apart from MNT curves): the Freeman curves and the Barreto–Naehrig curves. We prove that cycles within each of these families do not exist (section 8). This means that if one wants to obtain cycles from curve families, one must consider combinations of current families (or study future constructions of prime-order elliptic curves).

Overall, cycles of pairing-friendly elliptic curves seem much harder to understand, and to construct, than cycles of arbitrary elliptic curves. While our results have for the most part established limitations of pairing-friendly cycles, our outlook is optimistic. Our work demonstrates that studying pairing-friendly cycles is tractable and, moreover, points the way to concrete research questions that could lead to more tools for studying these cycles. We thus conclude the introduction with a selection of open problems.

1.2. Open problems.

1. Do there exist cycles consisting of elliptic curves with the *same* embedding degree? The varying embedding degrees in current constructions of cycles is inconvenient because, in practice, curves in the cycle have different security levels.
2. Can we construct cycles of embedding degrees greater than 6? All known pairing-friendly cycles involve embedding degrees at most 6, which means that it is inefficient to use such cycles at high security levels (e.g., 128 bits of security). It would be desirable to construct, or rule out, cycles of higher embedding degrees (say, 20).
3. In particular, can we construct 2-cycles of higher embedding degrees? Our technique for ruling out pairs with embedding degrees $(5, 10)$, $(8, 8)$, or $(12, 12)$ sheds some light on other pairs (k_1, k_2) for which $\Phi_{k_1}(x) = \Phi_{k_2}(-x)$, but it does not seem to extend to the case $\deg \Phi_{k_1}(x) > 4$. We believe that it would be especially interesting to study pairs with embedding degrees $(16, 16)$, which have cyclotomic polynomial $x^8 + 1$.
4. Do there exist cycles consisting of elliptic curves with the same discriminant and the same embedding degrees? Our work demonstrates that sharing the same discriminant is already quite limiting, and it would be interesting to understand how this

requirement interacts with that of sharing the same embedding degree.

5. Are there cycles from combinations of MNT, Freeman, and Barreto–Naehrig curves? Our preliminary investigations via Gröbner bases suggest small cycles are unlikely, but the question remains open for arbitrary-length cycles.

2. Preliminaries.

2.1. Elliptic curves and pairings. Let E be an elliptic curve over a finite field $\mathbb{F}_q$, where q is a prime. We denote this by $E/\mathbb{F}_q$, and we denote by $E(\mathbb{F}_q)$ the group of points of E over $\mathbb{F}_q$, with order $n = \#E(\mathbb{F}_q)$. The *trace* of $E/\mathbb{F}_q$ is $t = q + 1 - n$. By Hasse's theorem [32, Theorem V.1.1], t satisfies $|t| \leq 2\sqrt{q}$. We say that E is *supersingular* if $t \equiv 0 \pmod{q}$; otherwise E is *ordinary.*

The *endomorphism ring* $\mathrm{End}(E)$ of E consists of morphisms from E to itself that are also group homomorphisms on its points. If E is supersingular, then $\mathrm{End}(E)$ is an order in a quaternion algebra. If E is ordinary, then $\mathrm{End}(E)$ is an order in an imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$, for some positive squarefree integer D. We call D the *discriminant*, and we say that E has *complex multiplication* in $\mathbb{Q}(\sqrt{-D})$.[1]

Let $r \geq 2$ be an integer relatively prime to q. We denote the r-torsion points of E by $E[r]$, and we denote the group of rth roots of unity in the algebraic closure of $\mathbb{F}_q$ by μ_r. The *Weil pairing* is a bilinear nondegenerate map

$$e_r \colon E[r] \times E[r] \to \mu_r \,. \tag{2.1}$$

The *embedding degree* with respect to r is the smallest integer k such that r divides $q^k - 1$. In the case of prime-order curves, if $r = n$, we simply say that E has embedding degree k.

The Weil pairing was first used in cryptography to reduce the discrete logarithm problem on $E[r]$ to a discrete logarithm problem in μ_r, which is contained in $\mathbb{F}_{q^k}^*$ [24, 19]. Subsequently, starting with the work of [8, 21], the Weil pairing was used to achieve numerous cryptographic capabilities. For security, it is necessary to choose the embedding degree k such that the discrete logarithm problem in $\mathbb{F}_{q^k}^*$ is computationally infeasible. On the other hand, the embedding degree cannot be too large, or the computation of the Weil pairing (which grows linearly in k) would not be efficient enough for cryptographic applications.

We say that an elliptic curve $E/\mathbb{F}_q$ is *pairing-friendly* if $E(\mathbb{F}_q)$ has a large prime-order subgroup, and if the embedding degree is small (see [18] for a more precise definition). A random elliptic curve has a large embedding degree and thus is not pairing-friendly. Constructing pairing-friendly curves with specified parameters is a difficult problem with strong practical motivations that has been extensively studied. It was shown in [24] that supersingular elliptic curves can have embedding degree at most 6, and if the characteristic of q is not 2 or 3, the embedding degree is at most 3. As we are interested in large values of q and higher values of k for applications in cryptography, we focus on ordinary elliptic curves.

The known methods to construct ordinary pairing-friendly curves proceed by first finding parameters q, r, t, k such that there exists an elliptic curve $E/\mathbb{F}_q$ with trace t, a prime-order subgroup of size r, and embedding degree k. The *complex multiplication method* is then used to find the equation of the curve. This works if the *CM equation* $4q - t^2 = Dy^2$ has a solution

[1] Some works use the convention that D is negative. Throughout this work we take D to be positive.

with $y \in \mathbb{Z}$ and small positive discriminant $D \in \mathbb{Z}$. Indeed, state-of-the-art algorithms run in time $O(D \operatorname{polylog} D)$ and are only feasible for D of size up to 10^{16} [35].

It is useful to view the condition on the embedding degree via cyclotomic polynomials. Let Φ_m be the mth cyclotomic polynomial (the minimal polynomial over the rationals of an irreducible mth root of unity). It is known that (see, for example, [37])

$$x^m - 1 = \prod_{d|m} \Phi_d(x) . \tag{2.2}$$

Lemma 2.1. *Let $E/\mathbb{F}_q$ have prime order n. Then E has embedding degree k if and only if k is minimal such that n divides $\Phi_k(q)$.*

Proof. The condition that k is the embedding degree implies that k is minimal such that $q^k \equiv 1 \pmod n$. Using basic results on cyclotomic polynomials (see [37, Lemma 2.9]), this is equivalent to the condition that $n|\Phi_k(q)$. ■

This can be converted into a result relating n to the trace t.

Lemma 2.2 (see [2]). *$E/\mathbb{F}_q$ has embedding degree k if and only if $n|\Phi_k(t-1)$ and $n \nmid \Phi_i(t-1)$ for all $0 < i < k$.*

2.2. Families of pairing-friendly elliptic curves. We consider families of pairing-friendly elliptic curves with a fixed embedding degree, whose parameters are defined by polynomials. These are useful for generating curves for applications where curves of arbitrary size are desired. Each family is parametrized by polynomials $(q_k(x), n_k(x), t_k(x))$, representing the field of definition, number of rational points, and trace, respectively, where k is the embedding degree. These have to satisfy that $n_k(x) = q_k(x) + 1 - t_k(x)$, $n_k(x)$ divides $\Phi_k(t_k(x) - 1)$, and there must be infinitely many integer solutions (x, y) to the CM equation $4q_k(x) - t_k(x)^2 = Dy^2$, for some small positive discriminant $D \in \mathbb{Z}$.

Miyaji, Nakabayashi, and Takano [27] characterized all families of ordinary prime-order elliptic curves with embedding degrees $k = 3, 4, 6$. For these embedding degrees, the cyclotomic polynomial is quadratic, and the CM equation can be transformed into a generalized Pell equation. These families are parametrized by the polynomials in Table 2.1. We refer to elliptic curves belonging to the MNT families in Table 2.1 as *MNT curves.*

Table 2.1
MNT curves.

k	$q_k(x)$	$n_k(x)$	$t_k(x)$
3	$12x^2 - 1$	$12x^2 - 6x + 1$	$6x - 1$
4	$x^2 + x + 1$	$x^2 + 2x + 2$, $x^2 + 1$	$-x$, $x + 1$
6	$4x^2 + 1$	$4x^2 + 2x + 1$	$-2x + 1$

For other embedding degrees, there is no analogous characterization of all elliptic curves with a given embedding degree. Moreover, there is currently no method to construct families of prime-order elliptic curves of arbitrary embedding degrees. (If we allow for composite orders, there are algorithms to construct elliptic curves of arbitrary embedding degrees [12, 15].) There are two other constructions of prime-order families stated below.

Freeman [17] has constructed a family of prime-order elliptic curves with $k = 10$, which is parametrized by the following polynomials:

$$q_{10}(x) = 25x^4 + 25x^3 + 25x^2 + 10x + 3\,, \tag{2.3a}$$

$$n_{10}(x) = 25x^4 + 25x^3 + 15x^2 + 5x + 1\,, \tag{2.3b}$$

$$t_{10}(x) = 10x^2 + 5x + 3\,. \tag{2.3c}$$

Barreto and Naehrig [3] have another construction with $k = 12$, parametrized by

$$q_{12}(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1\,, \tag{2.4a}$$

$$n_{12}(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1\,, \tag{2.4b}$$

$$t_{12}(x) = 6x^2 + 1\,. \tag{2.4c}$$

Other constructions of pairing-friendly elliptic curves have *composite* orders. These include the families of Brezing and Weng [11] and of Barreto, Lynn, and Scott [2].

3. Cycles of pairing-friendly elliptic curves. In this paper we study cycles of pairing-friendly elliptic curves. This notion was introduced in [4] for applications in cryptography. We restate Definition 1.1 below.

Definition 3.1. *An* m-cycle of elliptic curves *is a list of* m *distinct elliptic curves* $E_1/\mathbb{F}_{q_1}$, $\ldots$, $E_m/\mathbb{F}_{q_m}$, *where* $q_1, \ldots, q_m$ *are prime, such that the numbers of points on these curves satisfy*

$$\#E_1(\mathbb{F}_{q_1}) = q_2\,, \ldots, \#E_i(\mathbb{F}_{q_i}) = q_{i+1}\,, \ldots, \#E_m(\mathbb{F}_{q_m}) = q_1\,. \tag{3.1}$$

Cryptographic applications require curves in the cycle to have small embedding degree.

Definition 3.2. *A* $(k_1, \ldots, k_m)$-cycle *is an* m*-cycle of distinct ordinary elliptic curves* $E_1/\mathbb{F}_{q_1}$, $\ldots$, $E_m/\mathbb{F}_{q_m}$ *such that* $E_i/\mathbb{F}_{q_i}$ *has embedding degree* k_i*, for each* $i = 1, \ldots, m$. *A* $(k_1, \ldots, k_m)$*-cycle is* pairing-friendly *if all the* k_i*'s are small (recall Definition 1.2).*

An m-cycle is a special case of a $(k_1, \ldots, k_m)$-cycle where the k_i's are arbitrary positive integers (or possibly infinity).

If we require that $q_1, \ldots, q_m$ are *distinct* primes, Definition 3.1 is equivalent to the notion of *aliquot cycles* for elliptic curves $E/\mathbb{Q}$ by Silverman and Stange [33]. An aliquot m-cycle for $E/\mathbb{Q}$ is a sequence of distinct primes $(q_1, \ldots, q_m)$ such that E has good reduction at each prime, and if we denote the reduction of E at q_i by $\tilde{E}_{q_i}$, then

$$\#\tilde{E}_{q_1}(\mathbb{F}_{q_1}) = q_2\,, \ldots, \#\tilde{E}_{q_i}(\mathbb{F}_{q_i}) = q_{i+1}\,, \ldots, \#\tilde{E}_{q_m}(\mathbb{F}_{q_m}) = q_1\,. \tag{3.2}$$

Given an aliquot m-cycle, we can construct an m-cycle of elliptic curves by setting $E_i := \tilde{E}_{q_i}$ for each i. Conversely, given an m-cycle where $q_1, \ldots, q_m$ are distinct, we can construct a curve $E/\mathbb{Q}$ by computing its coefficients via the Chinese remainder theorem in such a way that E's reduction at each q_i is E_i.

It is known that cycles of arbitrary lengths exist, just based on the Hasse bound and the fact that every trace in the Hasse bound is realized by an elliptic curve [14].

Proposition 3.3 (see [33, Theorem 5.1]). *For every $m \geq 1$ there exists an elliptic curve $E/\mathbb{Q}$ with an aliquot m-cycle.*

However, the foregoing result does not take into account the embedding degrees of the curves. In particular, it is not known if pairing-friendly cycles of arbitrary lengths exist.

The focus of this paper is the study of *pairing-friendly* cycles of elliptic curves. This is a significantly more restrictive notion than the aliquot cycles introduced in [33], since a random elliptic curve would not have a small embedding degree. Moreover, there are only a few known families of prime-order elliptic curves with small embedding degrees (see subsection 2.2 for a list of all such families). Even without the condition that the curves form a cycle, it is already a difficult problem to construct pairing-friendly elliptic curves of prime order.

We list below a few observations that we will use in this paper. First, the lemma below implies that to construct cycles of elliptic curves for applications (where the size of the finite fields tend to be large), we need only consider *ordinary* elliptic curves.

Lemma 3.4. *Let $E_1/\mathbb{F}_{q_1}, \ldots, E_m/\mathbb{F}_{q_m}$ be an m-cycle of elliptic curves, where $q_1, \ldots, q_m \geq 5$ are prime. Then all the curves must be ordinary elliptic curves.*

Proof. It is known that for any elliptic curve $E/\mathbb{F}_q$ with $q \geq 5$ prime, E is supersingular if and only if $\#E(\mathbb{F}_q) = q + 1$; see, for example, [32, Exercise 5.10]. Suppose $E_i/\mathbb{F}_{q_i}$ is supersingular for some i; then $\#E(\mathbb{F}_{q_i}) = q_i + 1 = q_{i+1}$. But since q_i is prime, $q_i + 1$ is even; hence this cannot hold. ∎

Next, we present a necessary condition for m elliptic curves to form an m-cycle. This condition is *not* sufficient as every trace in the Hasse interval can be realized by an elliptic curve [14]; hence this condition is not a strong restriction on the curves in the cycle.

Lemma 3.5. *Let $E_1/\mathbb{F}_{q_1}, \ldots, E_m/\mathbb{F}_{q_m}$ be an m-cycle of elliptic curves, with traces $t_1, \ldots, t_m$, respectively. Then the sum of their traces satisfies*

$$t_1 + \cdots + t_m = m\,. \tag{3.3}$$

Proof. Let $n_i = \#E_i(\mathbb{F}_{q_i})$, for each $i = 1, \ldots, m$. Since the curves form a cycle, we have the constraints $n_1 = q_2, \ldots, n_i = q_{i+1}, \ldots, n_m = q_1$. If we sum up these m equations, we get $n_1 + \cdots + n_m = q_1 + \cdots + q_m$. Using the fact that $n_i = q_i + 1 - t_i$, we get $t_1 + \cdots + t_m = m$. ∎

4. MNT cycles. We consider pairing-friendly cycles consisting of MNT curves (see Table 2.1), which are the ordinary prime-order elliptic curves of embedding degrees $3, 4, 6$. For brevity, we use the term *MNT cycles* for cycles where every curve is an MNT curve.

In [22, 4], MNT curves were used to give the first construction of pairing-friendly 2-cycles. In this section, we construct MNT 4-cycles, and characterize the possible MNT cycles.

Proposition 4.1. *All MNT cycles have lengths 2 or 4, and they are either $(6, 4)$-cycles or $(6, 4, 6, 4)$-cycles.*

The proof of this result proceeds in a few steps. First, in Lemma 4.2 we show that no curve in an MNT cycle can have embedding degree 3. Then, in Lemmas 4.4 and 4.5 we show that no two consecutive curves in an MNT cycle can both have embedding degree 4 or 6. Finally, we consider MNT cycles with alternating embedding degrees 4 and 6, and we show that these can only have length 2 or 4.

Lemma 4.2. *Let $E_1/\mathbb{F}_{q_{k_1}(x_1)}, \ldots, E_m/\mathbb{F}_{q_{k_m}(x_m)}$ be an MNT cycle, with $x_1, \ldots, x_m \in \mathbb{Z}$ and embedding degrees $k_1, \ldots, k_m \in \{3, 4, 6\}$. Then none of the embedding degrees can be 3.*

To show Lemma 4.2, we make use of the following result.

Lemma 4.3 (see [37, Proposition 2.10]). *Let q be a prime such that $q \nmid k$. Then q divides $\Phi_k(a)$ for some $a \in \mathbb{Z}$ if and only if $q \equiv 1 \pmod{k}$.*

Proof of Lemma 4.2. By Lemma 2.1, the condition that $E_i/\mathbb{F}_{q_{k_i}(x_i)}$ has embedding degree k_i implies that $n_{k_i}(x_i) \mid \Phi_{k_i}(q_{k_i}(x_i))$. Since $n_{k_i}(x_i) = q_{k_{i+1}}(x_{i+1})$, Lemma 4.3 implies

$$q_{k_{i+1}}(x_{i+1}) \equiv 1 \pmod{k_i}. \tag{4.1}$$

Suppose that $k_j = 3$ for some j. From Table 2.1,

$$q_3(x_j) = 12x_j^2 - 1 \equiv 1 \pmod{k_{j-1}}. \tag{4.2}$$

However, this is not possible since $12x_j^2 - 1 \equiv -1 \pmod{3, 4, 6}$. ∎

We show that for any MNT cycle, no two consecutive curves can both have embedding degree 4 or 6.

Lemma 4.4. *Let $E_1/\mathbb{F}_{q_{k_1}(x_1)}, \ldots, E_m/\mathbb{F}_{q_{k_m}(x_m)}$ be an MNT cycle, with $x_1, \ldots, x_m \in \mathbb{Z}$. Then no two consecutive curves can both have embedding degree 4.*

Proof. Suppose to the contrary that $k_i = k_{i+1} = 4$ for some i. Then $n_4(x_i) = q_4(x_{i+1})$. From Table 2.1, $q_4(x_{i+1}) = x_{i+1}^2 + x_{i+1} + 1$, and there are two possibilities for $n_4(x_i)$.

Suppose $n_4(x_i) = x_i^2 + 2x_i + 2$. Then $x_i^2 + 2x_i + 2 = x_{i+1}^2 + x_{i+1} + 1$, which implies

$$(x_i + 1)^2 = x_{i+1}(x_{i+1} + 1). \tag{4.3}$$

This is a contradiction if $x_i \neq -1$, since the product of two consecutive nonzero integers is not a square.[2] But if $x_i = -1$, then $n_4(x_i) = 1$ would not be prime.

Suppose $n_4(x_i) = x_i^2 + 1$. Then $x_i^2 + 1 = x_{i+1}^2 + x_{i+1} + 1$, which implies

$$x_i^2 = x_{i+1}(x_{i+1} + 1). \tag{4.4}$$

This is a contradiction by the same argument as above. ∎

Lemma 4.5. *Let $E_1/\mathbb{F}_{q_{k_1}(x_1)}, \ldots, E_m/\mathbb{F}_{q_{k_m}(x_m)}$ be an MNT cycle with $x_1, \ldots, x_m \in \mathbb{Z}$. Then no two consecutive curves can both have embedding degree 6.*

Proof. Suppose to the contrary that $k_i = k_{i+1} = 6$ for some i. Then $n_6(x_i) = q_6(x_{i+1})$. From Table 2.1, $q_6(x_{i+1}) = 4x_{i+1}^2 + 1$, and $n_6(x_i) = 4x_i^2 + 2x_i + 1$. Thus $4x_i^2 + 2x_i + 1 = 4x_{i+1}^2 + 1$, which implies

$$2x_i(2x_i + 1) = (2x_{i+1})^2. \tag{4.5}$$

This is a contradiction if $x_{i+1} \neq 0$, since the product of two consecutive nonzero integers is not a square. But if $x_{i+1} = 0$, then $q_6(x_{i+1}) = 1$ would not be prime. ∎

[2] Suppose that for some nonzero $x, y \in \mathbb{Z}$, $x(x+1) = y^2$. If $x > 0$, then $x^2 < y^2 < (x+1)^2$, which has no integer solutions for x, y. If $x < 0$, then $x^2 > y^2 > (x+1)^2$, which also has no integer solutions for x, y.

Table 4.1
MNT $(6, 4)$*-cycles.*

	E_1	E_2
k	6	4
$q(x)$	$4x^2+1$	$4x^2+2x+1$
$n(x)$	$4x^2+2x+1$	$4x^2+1$
$t(x)$	$-2x+1$	$2x+1$

We now consider MNT cycles consisting of elliptic curves with alternating embedding degrees 4 and 6.

Lemma 4.6. *Let $E_i/\mathbb{F}_{q_4}(x_i)$, $E_{i+1}/\mathbb{F}_{q_6}(x_{i+1})$ be consecutive curves in an MNT cycle. Then $2|x_{i+1}| = |x_i|$ or $2|x_{i+1}| = |x_i + 1|$.*

Proof. We have the condition $n_4(x_i) = q_6(x_{i+1})$. By Table 2.1, $q_6(x_{i+1}) = 4x_{i+1}^2 + 1$, and there are two possibilities for $n_4(x_i)$.

If $n_4(x_i) = x_i^2 + 2x_i + 2$, then $x_i^2 + 2x_i + 2 = 4x_{i+1}^2 + 1$, which we simplify to $(x_i + 1)^2 = (2x_{i+1})^2$. Thus $2|x_{i+1}| = |x_i + 1|$.

If instead $n_4(x_i) = x_i^2 + 1$, then $x_i^2 + 1 = 4x_{i+1}^2 + 1$, which we simplify to $x_i^2 = (2x_{i+1})^2$. Thus $2|x_{i+1}| = |x_i|$. ∎

Lemma 4.7. *Let $E_i/\mathbb{F}_{q_6}(x_i)$, $E_{i+1}/\mathbb{F}_{q_4}(x_{i+1})$ be consecutive curves in an MNT cycle. Then $x_{i+1} = 2x_i$.*

Proof. We have the condition $n_6(x_i) = q_4(x_{i+1})$. By Table 2.1, this gives $4x_i^2 + 2x_i + 1 = x_{i+1}^2 + x_{i+1} + 1$ or $2x_i(2x_i + 1) = x_{i+1}(x_{i+1} + 1)$. This implies $x_{i+1} = 2x_i$. ∎

We now prove Proposition 4.1 which states that all MNT cycles are $(6, 4)$-cycles or $(6, 4, 6, 4)$-cycles.

Proof of Proposition 4.1. By Lemmas 4.2, 4.4, and 4.5, all MNT cycles consist of curves with embedding degrees alternating between 4 and 6, and have even lengths.

Let $E_1/\mathbb{F}_{q_6}(x_1), E_2/\mathbb{F}_{q_4}(x_2), \ldots, E_{2m}/\mathbb{F}_{q_4}(x_{2m})$ be an MNT cycle. We first observe that Lemmas 4.6 and 4.7 imply that $|x_1| = |x_3| = \cdots = |x_{2m-1}|$. Thus $q_6(x_1) = q_6(x_3) = \cdots = q_6(x_{2m-1})$. As there are only two possibilities for $n_6(x_1), n_6(x_3), \ldots, n_6(x_{2m-1})$, for the curves to be distinct we must have $m \leq 4$, and if $m = 4$, then we must have $x_3 = -x_1$.

Let $x := x_1$. Then Lemma 4.7 implies $x_2 = 2x$. By Lemma 4.6, either $x_3 = x$, in which case we have a $(6, 4)$-cycle, or $x_3 = -x$. For the latter case, Lemma 4.7 implies that $x_4 = -2x$, which gives us a $(6, 4, 6, 4)$-cycle.

By substituting the possible parameter values for x into the polynomials in Table 2.1, we obtain the parametrizations of the possible families of MNT $(6, 4)$-cycles in Table 4.1 and $(6, 4, 6, 4)$-cycles in Table 4.2. These cycles can be constructed by substituting integer values of x and checking if all the $n(x)$'s and $q(x)$'s are prime. ∎

The MNT $(6, 4, 6, 4)$-cycles in Table 4.2 are unions of two MNT $(6, 4)$-cycles. Indeed, the pairs (E_1, E_2) and (E_3, E_4) each form $(6, 4)$-cycles. Furthermore, E_1, E_3 are defined over the same finite field. Interestingly, these are the only possible MNT 4-cycles, and no longer cycles consisting of distinct elliptic curves can be obtained by taking unions of MNT 2-cycles.

Table 4.2
MNT $(6,4,6,4)$*-cycles.*

	E_1	E_2	E_3	E_4
k	6	4	6	4
$q(x)$	$4x^2+1$	$4x^2+2x+1$	$4x^2+1$	$4x^2-2x+1$
$n(x)$	$4x^2+2x+1$	$4x^2+1$	$4x^2-2x+1$	$4x^2+1$
$t(x)$	$-2x+1$	$2x+1$	$2x+1$	$-2x+1$

Example 4.8. We give an example of an MNT $(6,4)$-cycle, using the parametrization in Table 4.1. If $x=1$, we check that $4x^2+1=5$ and $4x^2-2x+1=3$ are prime. We compute each of the two curves in the cycle using the CM method and Sage [36]:

$$E_1/\mathbb{F}_5 \,:\, y^2 = x^3 + 4x + 2\,, \tag{4.6a}$$

$$E_2/\mathbb{F}_3 \,:\, y^2 = x^3 + 2x^2 + 1\,. \tag{4.6b}$$

We list all the points of these curves in Table A.1.

Example 4.9. We give an example of an MNT $(6,4,6,4)$-cycle, using the parametrization in Table 4.2. If $x=3$, we check that $4x^2+1=37$, $4x^2+2x+1=43$, and $4x^2-2x+1=31$ are all prime. We compute the curves using Sage [36]:

$$E_1/\mathbb{F}_{37} \,:\, y^2 = x^3 + 24x + 16\,, \tag{4.7a}$$

$$E_2/\mathbb{F}_{43} \,:\, y^2 = x^3 + 36x + 5\,, \tag{4.7b}$$

$$E_3/\mathbb{F}_{37} \,:\, y^2 = x^3 + 22x + 27\,, \tag{4.7c}$$

$$E_4/\mathbb{F}_{31} \,:\, y^2 = x^3 + 26x + 21\,. \tag{4.7d}$$

We list all the points of these curves in Table A.2.

5. Two-cycles of specific embedding degrees. In this section we prove the following result.

Proposition 5.1. *There are no* $(5,10)$-*,* $(8,8)$-*, or* $(12,12)$*-cycles.*

The pairs $(5,10),(8,8),(12,12)$ are precisely the pairs (k_1,k_2) whose cyclotomic polynomials satisfy $\Phi_{k_1}(x)=\Phi_{k_2}(-x)$ and $\deg\Phi_{k_1}(x)=4$. To prove Proposition 5.1, we first use these conditions to reduce from the problem of classifying (k_1,k_2)-cycles to that of finding integral points on a few quartic curves, with finitely many exceptions, in Lemma 5.3. We then classify all integral points on these quartic curves and the finitely many exceptions using computational tools, yielding no actual (k_1,k_2)-cycles.

Note that in the case of 2-cycles, when we require nontrivial embedding degrees, the two curves cannot have equal field sizes.[3]

We first prove the following more general result, which we hope will also have applications to other kinds of 2-cycles.

[3] Even when allowed, curves $E/\mathbb{F}_q$ with $q=\sharp E(\mathbb{F}_q)$, known as *anomalous*, are undesirable because discrete logarithms can be computed in polynomial time via the SSSA attack [31, 34, 30].

Lemma 5.2. *Let* (k_1, k_2) *satisfy* $\Phi_{k_1}(x) = \Phi_{k_2}(-x)$. *Let* $E_1/\mathbb{F}_{q_1}, E_2/\mathbb{F}_{q_2}$ *be a* (k_1, k_2)*-cycle with* $q_1 > q_2$, *and let* $c = q_1 - q_2$. *Then* $q_1 q_2 \mid \Phi_{k_1}(c)$. *Additionally, for some integer* d *whose prime divisors are all congruent to* $1 \pmod{k_1}$, *there is an integer* y *such that*

$$y^2 = c^2 d^2 + 4d\Phi_{k_1}(c)\,. \tag{5.1}$$

Proof. By Lemma 2.1, the condition that $E_1/\mathbb{F}_{q_1}$ has embedding degree k_1 implies that $q_2 \mid \Phi_{k_1}(q_1)$. Then $q_2 \mid \Phi_{k_1}(q_1 - q_2)$ as well. Similarly, $q_1 \mid \Phi_{k_2}(q_2 - q_1) = \Phi_{k_1}(q_1 - q_2)$. It follows that $q_1 q_2 \mid \Phi_{k_1}(q_1 - q_2) = \Phi_{k_1}(c)$ as q_1 and q_2 are distinct primes.

Then $dq_1 q_2 = \Phi_{k_1}(c)$ for some integer d. Using $q_1 = q_2 + c$, we can rewrite this as

$$dq_2^2 + cdq_2 - \Phi_{k_1}(c) = 0\,. \tag{5.2}$$

For this quadratic equation in q_2 to have an integral solution, the discriminant

$$c^2 d^2 + 4d\Phi_{k_1}(c) \tag{5.3}$$

must be a perfect square, so that there is a y satisfying (5.1).

Also, for any prime $p \mid d$, the above relation $dq_1 q_2 = \Phi_{k_1}(c)$ implies that $p \mid \Phi_{k_1}(c)$. Hence $p \equiv 1 \pmod{k_1}$ by Lemma 4.3. ∎

Lemma 5.3. *In the situation of Lemma 5.2, additionally let* $\deg \Phi_{k_1}(x) = 4$. *Equivalently, let* $(k_1, k_2) \in \{(5, 10), (8, 8), (10, 5), (12, 12)\}$. *Then* $c \le 82$ *or* $1 \le d \le 16$.

Proof. Let $c \ge 83$. Then $\Phi_{k_1}(c) > 0$, so the relation $dq_1 q_2 = \Phi_{k_1}(c)$ implies $d \ge 1$. Next, because $E_2/\mathbb{F}_{q_2}$ has q_1 points, the Hasse bound implies $|q_1 - (q_2 + 1)| \le 2\sqrt{q_2}$. Substituting $c = q_1 - q_2$ and rearranging shows $q_2 \ge (c-1)^2/4$. The same holds for q_1 since $q_1 > q_2$. Then, $dq_1 q_2 = \Phi_{k_1}(c)$ implies

$$d < 16 \frac{\Phi_{k_1}(c)}{(c-1)^4}\,. \tag{5.4}$$

For each $k_1 \in \{5, 8, 10, 12\}$, we find that for $c \ge 83$, the right-hand side is at most 17. Thus either $c \le 82$ or $1 \le d \le 16$. ∎

For each (k_1, k_2) listed in Lemma 5.3, using the fact $q_1, q_2 \mid \Phi_{k_1}(c)$ from Lemma 5.2, one can see that the case $c \le 82$ yields only finitely many (k_1, k_2)-cycles. Also, for each $1 \le d \le 16$ whose prime divisors are congruent to $1 \pmod{k_1}$, one can show that (5.1) defines a plane curve of genus 1 in the coordinates (c, y). Siegel's theorem [23, Theorem 8.2.4] implies that such a curve has only finitely many integral points; hence there are only finitely many (k_1, k_2)-cycles.

We now use computational tools to show that there are, in fact, no (k_1, k_2)-cycles.

Proof of Proposition 5.1. Using the fact $q_1, q_2 \mid \Phi_{k_1}(c)$ from Lemma 5.2, it is easy to enumerate all (k_1, k_2)-cycles which have $c \le 82$, for $(k_1, k_2) \in \{(5, 10), (8, 8), (10, 5), (12, 12)\}$. Doing so using Sage [36] reveals no such examples.

We now consider the case $d \le 16$. Restricting to values of d whose prime factors are all congruent to $1 \pmod{k_1}$, we are left with the cases shown in Table 5.1.

Table 5.1
Cases $((k_1, k_2), d)$ satisfying Lemma 5.3 when $c \geq 83$.

(k_1, k_2)	d
$(5, 10)$	11
$(10, 5)$	13
$(12, 12)$	13

In the case $(k_1, k_2) = (12, 12)$, $d = 13$, we can enumerate the integral points of (5.1) using Magma's `IntegralQuarticPoints` function [9]. Doing so gives no examples with $c \geq 83$.

When $(k_1, k_2) = (5, 10)$ or $(10, 5)$ and $d = 11$, Sage [36] finds that (5.1) has no solutions over the ring of integers modulo 16; hence it has no integral solutions. Thus these cases also give no examples. ∎

When $\deg \Phi_{k_1}(x) > 4$, the bound on d in (5.4) no longer converges to a finite value as $c \to \infty$, so we cannot reduce to finding integral points on a finite number of curves as above. It would be interesting to find more general arguments which work for higher-degree cyclotomic polynomials, such as the case of $(16, 16)$-cycles, where $\Phi_{k_1}(x) = \Phi_{k_2}(x) = x^8 + 1$.

6. Cycles with the same discriminant. In this section we show that if we construct cycles from elliptic curves of the same discriminant D, then the length of the cycle must be small. This implies that to construct elliptic curves from polynomial families, we cannot use families with a fixed discriminant. The results in this section are *independent* of the embedding degrees of the elliptic curves.

We first show that any 2-cycle of ordinary elliptic curves consists of curves with the same discriminant.

Proposition 6.1. *Let $E_1/\mathbb{F}_{q_1}, E_2/\mathbb{F}_{q_2}$ be a 2-cycle of ordinary elliptic curves. Then they both have the same discriminant for complex multiplication.*

Proof. Let t_i be the trace of E_i for each i. Then $q_2 = q_1 + 1 - t_1$ and $q_1 = q_2 + 1 - t_2$. This implies $t_1 + t_2 = 2$, and

$$4q_2 - t_2^2 = 4(q_1 + 1 - t_1) - (2 - t_1)^2 = 4q_1 - t_1^2\,.$$

The discriminant of E_i is the squarefree part of $4q_i - t_i^2$, so the two curves have the same discriminant. ∎

The converse is also true if $D > 3$, as shown in [33, Corollary 6.2] and [1, Theorem 3.4]. We present an adapted version of the proof below.

Proposition 6.2. *Let $D > 3$ be a squarefree integer such that $-D \equiv 0, 1 \pmod 4$. Suppose that we have an m-cycle of ordinary elliptic curves $E_1/\mathbb{F}_{q_1}, \ldots, E_m/\mathbb{F}_{q_m}$ such that each elliptic curve has discriminant D and $q_1, \ldots, q_m$ are distinct primes. Then $m \leq 2$.*

Proof. For each $i = 1, \ldots, m$, let $y_i \in \mathbb{Z}$ be such that the CM equation $4q_i - t_i^2 = Dy_i^2$ is satisfied. First, we note that if we fix q_i and D, the solution (t_i, y_i) to the CM equation is unique up to sign. This follows from the fact that, under our assumptions on D, the units in the ring of integers of $\mathbb{Q}(\sqrt{-D})$ are ± 1; hence if two elements have the same norm, then they differ by a multiple of ± 1.

Now let $E_i/\mathbb{F}_{q_i}$, $E_{i+1}/\mathbb{F}_{q_{i+1}}$ be two consecutive curves in the cycle. Since

$$4q_{i+1} - (t_i - 2)^2 = 4(q_{i+1} - 1 + t_i) - t_i^2 = 4q_i - t_i^2 = Dy_i^2\,, \tag{6.1}$$

thus $t_i - 2 = \pm t_{i+1}$ and $y_i = \pm y_{i+1}$, by the uniqueness of the solution to the CM equation.

Suppose that $m \geq 3$. Without loss of generality, assume that q_2 is the smallest prime in the cycle. Then $q_2 < q_1, q_3$. From the previous paragraph we also have $t_1 - 2 = \pm t_2$. We consider the two cases separately.

If $t_1 - 2 = t_2$, then $q_2 = q_1 - 1 - t_2$. So we have the inequalities $q_1 = q_2 + 1 + t_2 > q_2$ and $q_3 = q_2 + 1 - t_2 > q_2$. Hence $1 > t_2 > -1$ so $t_2 = 0$. But this implies that $q_1 = q_3$, which contradicts the assumption that the q_i's are distinct.

If $t_1 - 2 = -t_2$, then $q_2 = q_1 - 1 + t_2$, so $q_1 = q_2 + 1 - t_2 = q_3$. This again contradicts the assumption that the q_i's are distinct. ■

For the case where $D = 3$, we cite the following result from [1].

Proposition 6.3 (see [1, Theorem 3.4]). *Suppose that we have an m-cycle of ordinary elliptic curves $E_1/\mathbb{F}_{q_1}, \dots, E_m/\mathbb{F}_{q_m}$ such that each elliptic curve has discriminant D and $q_1, \dots, q_m$ are distinct primes. If $m \geq 3$, then $m = 6$ and $D = 3$.*

The results in this section show that to construct m-cycles of elliptic curves with a fixed discriminant D, either $m \leq 2$ or $m = 6$ and $D = 3$. This places a strong restriction on possible cycles, and implies that we cannot construct long cycles from a single family of elliptic curves with a fixed discriminant. For example, the Barreto–Naehrig curves [3] all have discriminant $D = 3$.

We also note that the results in this section do not depend on the embedding degrees of the elliptic curves. It remains an open question to understand how restricting the embedding degrees places further restrictions on the possible cycles.

7. Cycles with cofactors.

Allowing for nonprime orders gives greater flexibility in constructing elliptic curves, while still having relevance to cryptographic applications. While there are few embedding degrees that can be achieved by current constructions of prime-order curves, there are methods that achieve *arbitrary* embedding degrees for composite-order curves [12, 15]. While composite-order curves tend to be less preferable than prime-order curves in applications, they can still be practical and sometimes even preferable.[4]

Nevertheless, we show in this section that allowing for nonprime orders does not give us greater flexibility in constructing cycles. Our arguments in this section rely only on the Hasse bound and the constraints on the orders of the elliptic curves posed by the cycle condition.

Definition 7.1. *An m-*cycle of elliptic curves with cofactors *consists of m distinct elliptic curves $E_1/\mathbb{F}_{q_1}, \dots, E_m/\mathbb{F}_{q_m}$ such that for positive integer cofactors $h_1, \dots, h_m$,*

$$\#E_1(\mathbb{F}_{q_1}) = h_1 q_2\,, \dots, \#E_i(\mathbb{F}_{q_i}) = h_i q_{i+1}\,, \dots, \#E_m(\mathbb{F}_{q_m}) = h_m q_1\,. \tag{7.1}$$

[4] For example, Barreto–Lynn–Scott curves [2] are composite-order curves that, thanks to their high embedding degrees, enable efficient implementations at high-security levels. As another example, Edwards curves [16, 7, 5] are composite-order curves that, thanks to their complete formulas for addition, enable efficient implementations that resist various side channels (e.g., [6]).

If all the cofactors are 1, then Definition 7.1 reduces to Definition 1.1. We show that, for any $m > 1$, we cannot have m-cycles of elliptic curves with any nontrivial cofactor (and large orders). We deduce this by considering only the Hasse bound on the orders of the curves.

Proposition 7.2. *For all $m > 1$, there exists no m-cycle of elliptic curves having at least one nontrivial cofactor (greater than 1) if $q_1, \ldots, q_m > 12m^2$.*

Proof. We first prove this for the simpler case where $m = 2$. Suppose that we have a 2-cycle of elliptic curves $E_1/\mathbb{F}_{q_1}, E_2/\mathbb{F}_{q_2}$ with cofactors such that $\#E_1(\mathbb{F}_{q_1}) = h_1 q_2$, $\#E_2(\mathbb{F}_{q_2}) = h_2 q_1$. The Hasse bound for E_1 implies

$$q_1 + 1 - 2\sqrt{q_1} \leq h_1 q_2 \leq q_1 + 1 + 2\sqrt{q_1}\,. \tag{7.2}$$

We can express this as $(\sqrt{q_1} - 1)^2 \leq h_1 q_2 \leq (\sqrt{q_1} + 1)^2$. Applying the same argument to E_2, we get the following two inequalities:

$$\sqrt{q_1} - 1 \leq \sqrt{h_1 q_2} \leq \sqrt{q_1} + 1\,, \tag{7.3}$$

$$\sqrt{q_2} - 1 \leq \sqrt{h_2 q_1} \leq \sqrt{q_2} + 1\,. \tag{7.4}$$

We can then bound q_2 as follows:

$$\sqrt{h_1 q_2} \leq \frac{1}{\sqrt{h_2}}(\sqrt{q_2} + 1) + 1\,. \tag{7.5}$$

If $h_1 > 1$ or $h_2 > 1$, this implies that

$$\sqrt{q_2} \leq \frac{\sqrt{h_2} + 1}{\sqrt{h_1 h_2} - 1} \leq 1 + \frac{2}{\sqrt{h_1 h_2} - 1} < 3\,. \tag{7.6}$$

The same argument applies for bounding q_1. Hence for any 2-cycle with nontrivial cofactors, the elliptic curves must have small orders.

We now extend the argument above to m-cycles with cofactors for all $m > 2$. Suppose we have an m-cycle with cofactors $\#E_1(\mathbb{F}_{q_1}) = h_1 q_2\,, \#E_2(\mathbb{F}_{q_2}) = h_2 q_3\,, \ldots, \#E_m(\mathbb{F}_{q_m}) = h_m q_1$. Applying the same argument as before, we have the inequalities

$$\begin{aligned}
\sqrt{h_m q_1} &\leq \sqrt{q_m} + 1 && \text{(7.7a)}\\
&\leq \frac{1}{\sqrt{h_{m-1}}}(\sqrt{q_{m-1}} + 1) + 1\\
&\leq \frac{1}{\sqrt{h_{m-1} h_{m-2}}}(\sqrt{q_{m-2}} + 1) + \left(1 + \frac{1}{\sqrt{h_{m-1}}}\right)\\
&\vdots\\
&\leq \frac{1}{\sqrt{h_{m-1} \cdots h_1}}(\sqrt{q_1} + 1) + \left(1 + \frac{1}{\sqrt{h_{m-1}}} + \cdots + \frac{1}{\sqrt{h_{m-1} \cdots h_2}}\right). && \text{(7.7b)}
\end{aligned}$$

We simplify this to

$$\sqrt{q_1}\left(1 - \frac{1}{\sqrt{h_m \cdots h_1}}\right) \leq \frac{1}{\sqrt{h_m}} + \frac{1}{\sqrt{h_m h_{m-1}}} + \cdots + \frac{1}{\sqrt{h_m \cdots h_1}}\,. \tag{7.8}$$

If at least one of $h_1, \ldots, h_m$ is greater than 1, then we can bound q_1 as follows:

$$\sqrt{q_1} \leq \frac{m}{1 - \frac{1}{\sqrt{h_m \cdots h_1}}} \leq \frac{m}{1 - \frac{1}{\sqrt{2}}} = (2 + \sqrt{2})m\,. \tag{7.9}$$

The above argument applies for $q_2, \ldots, q_m$; hence $q_i \leq (2+\sqrt{2})^2 m^2 < 12m^2$ for each i. For cryptographic applications, we would require the elliptic curves to be defined over much larger fields than the size of the cycle, contrary to this bound. ■

8. Other cycles on parametrized families. We have shown in section 7 that it is not possible to construct cycles of elliptic curves with nontrivial cofactors (and large orders relative to cycle length). Hence cycles of elliptic curves must be assembled from *prime*-order elliptic curves. At present the only known families of *pairing-friendly* prime-order elliptic curves are the MNT curves for $k = 3, 4, 6$, Freeman curves for $k = 10$ [17], and Barreto–Naehrig curves for $k = 12$ [3]. Now we prove that we cannot construct cycles from just Freeman curves or from just Barreto–Naehrig curves.

Proposition 8.1. *There do not exist cycles consisting only of Freeman curves.*

Proof. Lemma 3.5 poses a restriction on the sum of the traces in a cycle. The trace of the Freeman curves is parametrized by $t(x) = 10x^2 + 5x + 3$ (see (2.3)). We note that $t(x) > 1$ for all $x \in \mathbb{R}$, since the discriminant of $t(x) - 1$ is -55. Hence the condition in Lemma 3.5 cannot be satisfied for cycles consisting only of Freeman curves. ■

Proposition 8.2. *There do not exist cycles consisting only of Barreto–Naehrig curves.*

Proof. We again use Lemma 3.5. The trace of the Barreto–Naehrig curves is parametrized by $t(x) = 6x^2 + 1$ (see (2.4)); hence if we have a family of elliptic curves consisting only of Barreto–Naehrig curves, then each trace has to be 1. So $x = 0$ and $q(x) = n(x) = 1$ for every curve in the cycle, which is impossible since $q(x)$ and $n(x)$ have to be prime. ■

We remark that the proof of Lemma 4.2 also shows that there do not exist cycles consisting of just Barreto–Naehrig curves and MNT curves of embedding degree 3.

For combinations of MNT, Freeman, and Barreto–Naehrig curves, we did a preliminary investigation using Gröbner bases to find solutions to the following system of polynomial equations in m variables $x_1, \ldots, x_m$, where $k_1, \ldots, k_m \in \{3, 4, 6, 10, 12\}$:

$$n_{k_1}(x_1) = q_{k_2}(x_2), \quad n_{k_2}(x_2) = q_{k_3}(x_3), \ldots, n_{k_m}(x_m) = q_{k_1}(x_1)\,. \tag{8.1}$$

For $m \leq 4$ we found that the ideals generated by these polynomials have dimension 0 apart from the MNT cycles in Proposition 4.1, implying that we cannot construct other families of cycles of length up to 4. We leave it as an open problem to construct cycles from combinations of these families, or to show that they do not exist.

Appendix A. Dual elliptic primes. In [25, 26], dual elliptic primes were introduced for applications in primality proving.

Definition A.1 (see [26, Definition 10]). *Two primes p, q are* dual elliptic primes associated *to an order $\mathcal{O} \subseteq \mathbb{Q}(\sqrt{-D})$ if there is a prime $\pi \in \mathcal{O}$ such that $p = \pi\overline{\pi}$ and $q = (\pi + \varepsilon)\overline{(\pi + \varepsilon)}$ with $\varepsilon = \pm 1$.*

Table A.1

Example of an MNT $(6, 4)$*-cycle.*

	E_1	E_2
	$y^2 = x^3 + 4x + 2$	$y^2 = x^3 + 2x^2 + 1$
(q, n, t, k, D)	$(5, 3, 3, 6, 11)$	$(3, 5, -1, 4, 11)$
points (excluding point at infinity)	(3,1) (3,4)	(0,1) (0,2) (1,1) (1,2)

Table A.2

Example of an MNT $(6, 4, 6, 4)$*-cycle.*

	E_1	E_2	E_3	E_4
	$y^2 = x^3 + 24x + 16$	$y^2 = x^3 + 36x + 5$	$y^2 = x^3 + 22x + 27$	$y^2 = x^3 + 26x + 21$
(q, n, t, k, D)	$(37, 43, -5, 6, 123)$	$(43, 37, 7, 4, 123)$	$(37, 31, 7, 6, 11)$	$(31, 37, -5, 4, 11)$
points (excluding point at infinity)	(0,4) (18,29) (0,33) (23,9) (1,2) (23,28) (1,35) (26,7) (3,2) (26,30) (3,35) (27,16) (4,18) (27,21) (4,19) (28,12) (7,3) (28,25) (7,34) (31,10) (9,6) (31,27) (9,31) (32,17) (12,16) (32,20) (12,21) (33,2) (13,3) (33,35) (13,34) (34,18) (14,5) (34,19) (14,32) (35,16) (17,3) (35,21) (17,34) (36,18) (18,8) (36,19)	(3,21) (23,10) (3,22) (23,33) (4,16) (29,5) (4,27) (29,38) (5,3) (30,7) (5,40) (30,36) (7,16) (31,9) (7,27) (31,34) (8,17) (32,16) (8,26) (32,27) (12,12) (33,8) (12,31) (33,35) (13,2) (38,1) (13,41) (38,42) (18,11) (41,21) (18,32) (41,22) (19,18) (42,21) (19,25) (42,22)	(0,8) (23,34) (0,29) (25,12) (3,3) (25,25) (3,34) (27,18) (5,15) (27,19) (5,22) (28,5) (8,7) (28,32) (8,30) (30,14) (10,10) (30,23) (10,27) (31,7) (11,3) (31,30) (11,34) (35,7) (12,13) (35,30) (12,24) (36,2) (23,3) (36,35)	(2,9) (18,11) (2,22) (18,20) (3,8) (20,4) (3,23) (20,27) (5,11) (21,1) (5,20) (21,30) (7,9) (22,9) (7,22) (22,22) (8,11) (23,13) (8,20) (23,18) (10,14) (26,13) (10,17) (26,18) (13,13) (27,15) (13,18) (27,16) (15,2) (28,3) (15,29) (28,28) (16,10) (30,5) (16,21) (30,26)

Dual elliptic primes are equivalent to 2-cycles of ordinary elliptic curves.

Proposition A.2. *Let p, q be dual elliptic primes associated to an order $\mathcal{O} \subseteq \mathbb{Q}(\sqrt{-D})$. Then p, q correspond bijectively to a 2-cycle of ordinary elliptic curves $E_1/\mathbb{F}_p, E_2/\mathbb{F}_q$ with complex multiplication by $\mathcal{O}$.*

Proof. Let p, q be dual elliptic primes. Then

$$q = (\pi + \varepsilon)\overline{(\pi + \varepsilon)} = p + \varepsilon(\pi + \overline{\pi}) + 1 \,. \tag{A.1}$$

Let $t_1 = -\varepsilon(\pi + \overline{\pi})$ and $t_2 = \varepsilon((\pi + \varepsilon) + \overline{(\pi + \varepsilon)})$. Then $q = p - t_1 + 1$ and $t_2 = -t_1 + 2$, so $p = q + 1 - t_2$. Thus the elliptic curves $E_1/\mathbb{F}_p, E_2/\mathbb{F}_q$ with traces t_1, t_2, respectively, form a 2-cycle. Moreover, since p, q are the norms of principal $\mathcal{O}$-ideals, these elliptic curves have complex multiplication by $\mathcal{O}$.

Conversely, let $E_1/\mathbb{F}_p, E_2/\mathbb{F}_q$ be a 2-cycle of ordinary elliptic curves with complex multiplication by $\mathcal{O}$. We can write the CM equations as $4p - t_1^2 = y^2 D$ and $4q - t_2^2 = y^2 D$. Let λ_1 be a root of $x^2 - t_1 x + p$, and let λ_2 be a root of $x^2 - t_2 x + q$, chosen such that

$$\lambda_1 = \frac{t_1 + y\sqrt{-D}}{2}, \tag{A.2}$$

$$\lambda_2 = \frac{t_2 - y\sqrt{-D}}{2}. \tag{A.3}$$

Then p, q are the norms of the principal $\mathcal{O}$-ideals $(\lambda_1), (\lambda_2)$, respectively. Since $t_2 = 2 - t_1$, we have $\lambda_2 = 1 - \lambda_1$. Let $\varepsilon = \pm 1$ and $\pi = -\varepsilon\lambda_1$. Then $p = \lambda_1\overline{\lambda_1} = \pi\overline{\pi}$ and $q = \lambda_2\overline{\lambda_2} = (\pi + \varepsilon)\overline{(\pi + \varepsilon)}$. ■

Acknowledgments. We thank Bernd Sturmfels for helpful comments. We also thank François Morain for informing us about the application of cycles of elliptic curves to primality proving. We thank Pierre Houedry for pointing out an error in a previous version of our paper.

REFERENCES

[1] L. Babinkostova, K. M. Bombardier, M. M. Cole, T. A. Morrell, and C. B. Scott, *Elliptic Reciprocity*, preprint, https://arxiv.org/abs/1212.1983, 2012.

[2] P. S. Barreto, B. Lynn, and M. Scott, *Constructing elliptic curves with prescribed embedding degrees*, in International Conference on Security in Communication Networks, Springer-Verlag, Berlin, Heidelberg, 2002, pp. 257–267.

[3] P. S. Barreto and M. Naehrig, *Pairing-friendly elliptic curves of prime order*, in International Workshop on Selected Areas in Cryptography, Springer-Verlag, Berlin, Heidelberg, 2005, pp. 319–331.

[4] E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza, *Scalable zero knowledge via cycles of elliptic curves*, in Proceedings of the 34th Annual International Cryptology Conference, CRYPTO '14, 2014, pp. 276–294; extended version available at http://eprint.iacr.org/2014/595.

[5] D. J. Bernstein, P. Birkner, M. Joye, T. Lange, and C. Peters, *Twisted Edwards curves*, in Proceedings of the 1st International Conference on Cryptology in Africa, AFRICACRYPT' 08, Springer-Verlag, Berlin, Heidelberg, 2008, pp. 389–405.

[6] D. J. Bernstein, N. Duif, T. Lange, P. Schwabe, and B.-Y. Yang, *High-speed high-security signatures*, in Proceedings of the 13th International Conference on Cryptographic Hardware and Embedded Systems, CHES '11, Springer, Berlin, Heidelberg, 2011, pp. 124–142.

[7] D. J. Bernstein and T. Lange, *Faster addition and doubling on elliptic curves*, in Proceedings of the 13th International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT '07, Springer, Berlin, Heidelberg, 2007, pp. 29–50.

[8] D. Boneh and M. K. Franklin, *Identity-based encryption from the Weil pairing*, SIAM J. Comput., 32 (2003), pp. 586–615, https://doi.org/10.1137/S0097539701398521.

[9] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system.* I. *The user language*, J. Symbolic Comput., 24 (1997), pp. 235–265, https://doi.org/10.1006/jsco.1996.0125.

[10] A. Breitman, *Scaling Tezos*, https://hackernoon.com/scaling-tezo-8de241dd91bd, 2017.

[11] F. Brezing and A. Weng, *Elliptic curves suitable for pairing based cryptography*, Des. Codes Cryptogr., 37 (2005), pp. 133–141.

[12] C. Cocks and R. Pinch, *Identity-based cryptosystems based on the Weil pairing*, unpublished manuscript, 2001.

[13] Coda, *Coda cryptocurrency protocol*, https://codaprotocol.com/, 2018.

[14] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ., 14 (1941), pp. 197–272.

[15] R. Dupont, A. Enge, and F. Morain, *Building curves with arbitrary small MOV degree over finite prime fields*, J. Cryptology, 18 (2005), pp. 79–89.

[16] H. M. Edwards, *A normal form for elliptic curves*, Bull. Amer. Math. Soc. (N.S.), 44 (2007), pp. 393–422.
[17] D. Freeman, *Constructing pairing-friendly elliptic curves with embedding degree* 10, in Algorithmic Number Theory, Lecture Notes in Comput. Sci. 4076, Springer, Berlin, 2006, pp. 452–465.
[18] D. Freeman, M. Scott, and E. Teske, *A taxonomy of pairing-friendly elliptic curves*, J. Cryptology, 23 (2010), pp. 224–280.
[19] G. Frey and H. Rück, *A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves*, Math. Comp., 62 (1994), pp. 865–874, https://doi.org/10.2307/2153546.
[20] N. Jones, *Elliptic aliquot cycles of fixed length*, Pacific J. Math., 263 (2013), pp. 353–371, https://doi.org/10.2140/pjm.2013.263.353.
[21] A. Joux, *A one round protocol for tripartite Diffie–Hellman*, J. Cryptology, 17 (2004), pp. 263–276.
[22] K. Karabina and E. Teske, *On prime-order elliptic curves with embedding degrees $k=3$, 4, and* 6, in Algorithmic Number Theory, A. J. van der Poorten and A. Stein, eds., Lecture Notes in Comput. Sci. 5011, Springer, Berlin, Heidelberg, 2008, pp. 102–117.
[23] S. Lang, *Fundamentals of Diophantine Geometry*, Springer-Verlag, New York, 1983, https://doi.org/10.1007/978-1-4757-1810-2.
[24] A. J. Menezes, T. Okamoto, and S. A. Vanstone, *Reducing elliptic curve logarithms to logarithms in a finite field*, IEEE Trans. Inform. Theory, 39 (1993), pp. 1639–1646, https://doi.org/10.1109/18.259647.
[25] P. Mihăilescu, *Cyclotomy of Rings & Primality Testing*, Ph.D. thesis, ETH Zürich, Zürich, Switzerland, 1997.
[26] P. Mihăilescu, *Dual Elliptic Primes and Applications to Cyclotomy Primality Proving*, preprint, https://arxiv.org/abs/0709.4113, 2007.
[27] A. Miyaji, M. Nakabayashi, and S. Takano, *New explicit conditions of elliptic curve traces for FR-reduction*, IEICE Trans. Fundam., 84 (2001), pp. 1234–1243.
[28] J. Parks, *Amicable pairs and aliquot cycles on average*, Int. J. Number Theory, 11 (2015), pp. 1751–1790, https://doi.org/10.1142/S1793042115500761.
[29] J. Parks, *An asymptotic for the average number of amicable pairs for elliptic curves*, Math. Proc. Cambridge Philos. Soc., 166 (2019), pp. 33–59, https://doi.org/10.1017/S0305004117000688.
[30] T. Satoh and K. Araki, *Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves*, Comment. Math. Univ. St. Paul., 47 (1998), pp. 81–92, https://ci.nii.ac.jp/naid/110007696197/en/.
[31] I. A. Semaev, *Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p*, Math. Comp., 67 (1998), pp. 353–356, https://doi.org/10.1090/S0025-5718-98-00887-4.
[32] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, Dordrecht, 2009.
[33] J. H. Silverman and K. E. Stange, *Amicable pairs and aliquot cycles for elliptic curves*, Exp. Math., 20 (2011), pp. 329–357.
[34] N. P. Smart, *The discrete logarithm problem on elliptic curves of trace one*, J. Cryptology, 12 (1999), pp. 193–196, https://doi.org/10.1007/s001459900052.
[35] A. V. Sutherland, *Accelerating the CM method*, LMS J. Comput. Math., 15 (2012), pp. 172–204, https://doi.org/10.1112/S1461157012001015.
[36] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version* 7.5.1*)*, 2017, http://www.sagemath.org.
[37] L. C. Washington, *Introduction to Cyclotomic Fields*, Grad. Texts in Math. 83, Springer-Verlag, New York, 1997.