

Revisiting cycles of pairing-friendly elliptic curves

Marta Bellés–Muñoz^{1,2}, Jorge Jiménez Urroz^{3,4}, Javier Silva¹

¹ Dusk Network, Netherlands,

² Pompeu Fabra University, Spain,

³ Polytechnic University of Catalonia, Spain,

⁴ Technical University of Madrid, Spain.

{marta, javier}@dusk.network, jorge.urroz@upc.edu

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. 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 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 [42,8]. Here, 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 require two things from the proof system. 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 [35,24,22], 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

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

is that they require a set of public parameters, 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 [10,11]. However, we focus on the case of pairing-based SNARKs, due to the appeal of constant-time verification.

1.1 Avoiding non-native arithmetic with cycles

A pairing-based 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. 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 [40]. Therefore, we shall assume that $p \neq q$. Another approach is to instantiate a new copy of the SNARK with another elliptic curve E' to deal with \mathbb{F}_q -circuits. In [14], 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 $p_1 \mid \#E_2(\mathbb{F}_{p_2})$.

A more ambitious approach, proposed in [8], is to use pairs of curves that also satisfy that $p_2 \mid \#E_1(\mathbb{F}_{p_1})$. 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 [39] 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 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 [13], the authors 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 [33], who characterized all prime-order curves with

embedding degrees 3, 4, and 6. These are called MNT curves. Based on the work from [23], Barreto and Naehrig [6] found a new family of curves with embedding degree 12, and later Freeman [18] found another one with embedding degree 10. The only known cycles are formed by alternating MNT curves of embedding degrees 4 and 6 [26,13]. 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 [31], 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, [13] suggests embedding degrees 12 or 20.

Chiesa, Chua, and Weidner [13] characterized all the possibilities for cycles consisting of MNT curves and 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 [17] but there are still some interesting problems in the direction of cycles. In particular, [13] 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 [13] 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 [13], 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 $k \leq 20$. 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. 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 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 [38, Theorem V.1.1] states that $|t| \leq 2\sqrt{q}$, and Deuring's theorem [15, 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*

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

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 m th 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 [38, §III.8] pairing. 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 $p \mid \Phi_k(q)$ [33, Remark 1].
- k is minimal such that $p \mid \Phi_k(t - 1)$ [5, Lemma 1].

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

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 [31] and [21] reductions. 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 $|d| \approx 10^{16}$ [41].

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 [33,6], but is studied in a more systematic way in [18,20]. 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 [36] 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 1. 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.

Let $f(X) = 4q(X) - t(X)^2$. Freeman [18] 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 .

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.

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 [38, 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, [18] also presents 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 $p \mid \Phi_k \circ t$, 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, [33], 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 Valena [23], two additional families were found: Barreto and Naehrig [6] found a family with $k = 12$, and Freeman [18] 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 1.

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 [19], 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 .

Require: Bound B on $|t_i|$ and target embedding degree k .

```

d = φ(k)/2
for (t0, ..., td) in [-B, B]d+1 do
  t = ∑i=0d tiXi
  for p | Φk(t - 1) do
    q = p - 1 + t
    if p or q do not represent primes then continue
    f = 4q - t2
    if deg f > 2 and f has no repeated roots then continue
  print (t, p, q)

```

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

Lemma 2.11 ([23], Lemma 1). *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) .

Proposition 2.12. *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} .*

Proof. 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

$$y^2 - \Delta^2 = 4a\zeta \tag{1}$$

over $K = \mathbb{Q}(\zeta)$. Raising Equation (1) to the k -th power, we get

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

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

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

If Equation (2) 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. \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 $\Phi_k\left(-\frac{\Delta^2}{4a}\right)$ 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 [39].

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

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

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

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 $E' \leftrightarrow (2 - t, q, p)$.
- p is in the Hasse interval of q if and only if q is in the Hasse interval of p . Indeed, if the former holds, we have that

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

which is equivalent to

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

It is known that cycles of any length exist [39, Theorem 11]. We summarize in the following two propositions some facts about cycles. These results are due to [13].

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 is no 2-cycle with embedding degree pairs $(5, 10)$, $(8, 8)$ or $(12, 12)$.
- (ii) There is no cycle formed only by Freeman curves.
- (iii) There 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 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 prime. Since they 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 $k = 1, 2, \ell, 2\ell$. We already know that $k \neq 1, 2$. Hence, $k = \ell$ or 2ℓ . But then $\ell \mid q - p$, and thus

$$|q - p| \geq \ell = \frac{p - 1}{2} > 2\sqrt{p} + 1$$

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

Proposition 3.6. *Let $s \in \mathbb{Z}$. Consider a family of elliptic curves with trace parameterized by a polynomial $t \in \mathbb{Q}[X]$, with $\deg t$ even. Then, only finitely many curves from this family form s -cycles within the family.*

Proof. If s curves with traces t_1, \dots, 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 $a, b \in \{1, \dots, s\}$ 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 in the polynomial case 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 $\Phi_k(x) = x^{\varphi(k)} + o(x^{\varphi(k)})$. More precisely, for $k \leq 104$, the k -th cyclotomic polynomial has only ± 1 as coefficients [32]. 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 $x \rightarrow -\infty$. The result follows directly from applying part (i) to $\Phi_k(x)$.

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.

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 $E \leftrightarrow (2 - t, q, p)$ be two elliptic curves with $|t| > 1$ and the same embedding degree $k \equiv 0 \pmod{4}$, such that $k \leq 3 \leq 104$. 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

$$\begin{aligned} p &\mid \Phi_k(t - 1), \\ q &\mid \Phi_k(1 - t), \end{aligned}$$

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.

Corollary 3.11. *Let $E \leftrightarrow (t, p, q)$ and $E \leftrightarrow (2 - t, q, p)$ be two elliptic curves with the same embedding degree $k \equiv 0 \pmod{4}$, such that $k \leq 3 \leq 104$. 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 $q > 15$. This shows that there are no $(4, 4)$ -cycles (which was already known from [13]).

– 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) $q \mid p^\ell - 1$, 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 . 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 1), we prove that no curve from them is part of a 2-cycle with any curve with embedding degree $\ell \leq 20$.

4.1 Cycles from parametric-families

First, we show a technique will that 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 $i = 0, \dots, \ell - 1$. Then, if a curve E from the family is in a cycle, the previous curve in the cycle does not have embedding degree ℓ .

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 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 $i = 0, \dots, \ell$. □

By testing the 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*

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

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

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

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 $[A, B]$, 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 $[A, B]$. For known families of curves, we will deal with the cases $x \in [A, B]$ 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 $x \in \mathbb{Z} \setminus [A, B]$, we have that either $r_x = cr(x)$ or $r_x = cr(x) + b(x)$. More precisely, let us denote $\sigma_A = \text{sign}\{r(x) \mid x < A\}$ and $\sigma_B = \text{sign}\{r(x) \mid x > B\}$, respectively. Then

$$r_x = \begin{cases} cr(x) + \left(\frac{1-\sigma_A}{2}\right)b(x) & \text{for } x < A, \\ cr(x) + \left(\frac{1-\sigma_B}{2}\right)b(x) & \text{for } x > B, \end{cases}$$

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 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 $0 \leq r_x < b(x)$, and $\deg r < \deg b$, and all these values are integer. Subtracting, we obtain

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

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

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

- Let $A \in \mathbb{Z}$ be the largest integer such that $0 < -cr(x) \leq b(x)$ for all $x < A$. Such A exists because both $b(x), -cr(x) \rightarrow \infty$ when $x \rightarrow -\infty$, and $\deg b > \deg(-cr)$. If $x < A$, 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 $B \in \mathbb{Z}$ be the smallest integer such that $0 \leq cr(x) < b(x)$ for all $x > B$. Such B exists because both $b(x), cr(x) \rightarrow \infty$ when $x \rightarrow \infty$, and $\deg b > \deg(cr)$. If $x > B$, 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 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 $c, A, B, \in \mathbb{Z}, \sigma_A, \sigma_B \in \{\pm 1\}$ such that, if $x < A$,

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

and if $x > B$, then

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

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

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 $q \nmid p^\ell - 1$ 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 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 are summarized in Table 2 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 $A = B = 0$, 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 $25aX^3 + 5bX^2 + 5cX + d$, 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

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

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 in MNT4 and MNT6 families are in stark contrast with the other families, but can be easily explained. In MNT3, BN and Freeman curves, the remainder r of the polynomial division q^k by p has coefficients that increase with k . Because of this, we need to get further away from zero before the asymptotic 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 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 $p^k \pmod{q}$ can only take 6 possible values. Concretely, $p(X)^k \pmod{q(X)} \in \{\pm 1, \pm X, \pm(X+1)\}$ for any $k \in \mathbb{N}$, and all of these yield the bounds $A = -1, B = 1$. Similarly, in the case of MNT6 curves, the remainder of p^k by q can only take 4 values. Concretely $p(X)^k \pmod{q(X)} \in \{\pm 1, \pm 2X\}$ for any $k \in \mathbb{N}$, which yield the bounds $A = B = 0$.

An exhaustive search in $[A, B]$ reveals no curves with embedding degree ℓ , for any of the values of ℓ considered.

Corollary 4.8. *Let (E, E') be a 2-cycle of elliptic curves, and assume that E' has embedding degree $\ell \leq 20$. Then:*

- (i) E is not an MNT curve, unless (E, E') is a cycle formed by an MNT4-MNT6 pair.
- (ii) E is not a Freeman curve.
- (iii) E is not a BN curve.

5 Probabilities and estimates

In this section, we generalize the results in [4] to s -cycles of elliptic curves. In particular, an s -cycle is a collection of s primes q_1, \dots, q_s and s elliptic curves $E_1/\mathbb{F}_{q_1}, \dots, E_s/\mathbb{F}_{q_s}$, such that $|E_i(\mathbb{F}_{q_i})| = q_{i+1 \pmod{s}}$. Among these, we are interested in estimating the probability of finding cycles 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, \dots, 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.

Theorem 5.1. *Let $s \geq 2$ and $X \in \mathbb{Z}$. Let \mathfrak{p} be the probability of finding an s -cycle of elliptic curves $(E_{q_1}, \dots, E_{q_s})$ with $q_i \in [X, 2X]$ and embedding degrees $k_i \leq K$ for all $i = 1, \dots, s$, by sampling uniformly from all the s -cycles of elliptic curves with orders in the interval $[X, 2X]$. Then*

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

for some constant c depending on s .

We first count the s -tuples of possible primes q_1, \dots, q_s .

Lemma 5.2. *Let $s \geq 2$ a positive integer fixed and $C > 0$ a constant depending on s . For any $X \geq 2$ we denote $T_s(X)$ the number of s -tuples of primes in the interval $[X, 2X]$ with $|q_i - q_j| \leq C\sqrt{X}$. Then, there exist constants c_1, c_2 depending on s , such that*

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

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

$$\sum_{k=1}^{\sqrt{X}/C} \pi_k = \pi(X_C) - \pi(X) = \frac{X}{\log X} + E,$$

where $|E| < \varepsilon \frac{X}{\log X}$ for any $\varepsilon > 0$ and $X > X_\varepsilon$ 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 $X > X_\varepsilon$

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

and hence

$$\frac{cX^{(s+1)/2}}{(\log X)^s} \leq \sum_{k=1}^{\sqrt{X}/C} \pi_k^s.$$

Finally observe that every s -tuple of primes on each interval I_k is counted in $T_s(X)$, so we will use the above to get a lower bound on $T_s(X)$. 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 inequality [34, Corollary 2]

$$\pi(M+N) - \pi(M) \leq \frac{2M}{\log M}, \quad (3)$$

we get $\pi_k \leq c \frac{\sqrt{X}}{\log X}$ for any k and hence

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

which gives us the bound

$$|A| > c\sqrt{X}$$

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

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

In order to prove the second inequality, we denote the primes in the interval $[X, 2X]$, 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 $I_i = (q_i, q_i + C\sqrt{X}]$. Hence, letting $\pi_i = \sum_{q \in I_i} 1$, we can apply the inequality (3) to obtain

$$T_s(X) \leq \sum_{i=1}^N \binom{\pi_i}{s-1} \leq c \sum_{i=1}^N \pi_i^{s-1} \leq c \frac{X^{\frac{s-1}{2}}}{(\log X)^{s-1}} N \leq c \frac{X^{\frac{s+1}{2}}}{(\log X)^s}. \quad (4)$$

Remark 5.3. For $s = 2$ and $C = 1$ we can get any constant $c_1 < 1/2$, by noting that

$$T_2(X) \geq \frac{1}{2} \sum_{k=1}^{\sqrt{X}} \pi_k (\pi_k - 1) = \frac{1}{2} \sum_{k=1}^{\sqrt{X}} \pi_k^2 - \frac{1}{2} \sum_{k=1}^{\sqrt{X}} \pi_k \geq \frac{1}{2} \frac{X^{3/2}}{(\log X)^2} - \frac{1}{2} \frac{X}{\log X} \geq \left(\frac{1}{2} - \varepsilon\right) \frac{X^{3/2}}{(\log X)^2}.$$

A different proof of the lower bound for the case $s = 2$ and $C = 1$, with a slightly worst constant, is given in [28, Lemma 1].

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

Lemma 5.4. *For any $X > 0$ and $K > 0$, let $T_{s,K}(X)$ be the number of s -tuples of primes in the interval $[X, 2X]$, with $|q_i - q_j| \leq C\sqrt{X}$, for some constant $C > 0$ and such that $q_{i+1} | q_i^{k_i} - 1$ for some $k_i \leq K$. Then*

$$T_{s,K}(X) \leq cK(K+1)\sqrt{X},$$

for some constant $c > 0$.

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

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

Lemma 5.5. *Let $C_s(X)$ the set 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 $C_{s,K}(X) \subset C_s(X)$ the subset in which E_i has embedding $k_i \leq K$ for all $i = 1, \dots, s$. Then*

$$c_1 K \frac{X^{(2s+1)/2}}{(\log X)^{2s}} \leq |C_s(X)| \leq c_2 K (\log \log X)^{2s} X^{(2s+1)/2}$$

$$|C_{s,k}(X)| \leq c_3 K (K+1) (\log X)^s (\log \log X)^{2s} X^{(s+1)/2}$$

for some constants c_1, c_2, c_3 depending on s .

Proof. First note that, if we have an s -cycle of curves, then the corresponding primes are as in Lemma 5.2 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 , 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

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

and then observe that the largest prime in the cycle can only be $s/2$ steps apart from the first one, since they form a cycle.

Now, let us start by proving the upper bound for $C_s(X)$. We know by [29, Proposition 1.9] that for every q and every subset of integers L such that for any $\ell \in L$, $|\ell - q + 1| \leq 2\sqrt{q}$, there are at most $c \log q (\log \log q)^2 \sqrt{q} |L|$ isomorphism classes over \mathbb{F}_q of elliptic curves with $|E(\mathbb{F}_q)| \subset L$ for some constant c , so on each s -tuple there will be less than

$$c (\log X)^s (\log \log X)^{2s} X^{s/2}$$

isomorphism classes of elliptic curves with points on the s -tuple and, in particular, forming a cycle of length at most s . Applying the second inequality of Lemma 5.2, we get the expected upper bound for cycles of length at most s , and in particular for $C_s(X)$.

Now, to prove the lower bound for $C_s(X)$ we see that the same Proposition 1.9 of [29] shows that for every subset of integers $L \subset [q - \sqrt{q}, q + \sqrt{q}]$ with $|L| \geq 3$ there are more than $c(|L| - 2) \frac{\sqrt{q}}{\log q}$ isomorphism classes over \mathbb{F}_q of elliptic curves with $|E(\mathbb{F}_q)| \subset S$ for some constant c , so on each s -tuple with $s \geq 3$ we have more than $c^s \frac{X^{s/2}}{(\log X)^s}$ isomorphism classes of elliptic curves with points on the s -tuple and, in particular, forming a cycle of length at most s . Combining this with the first inequality of Lemma 5.2, we get the lower bound

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

Then, $C_s(X)$ 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

$$C_s(X) \geq c \frac{X^{(2s+1)/2}}{(\log X)^{2s}} - c \frac{X^{(2s-1)/2}}{(\log X)^{2s-2}} \geq c \frac{X^{(2s+1)/2}}{(\log X)^{2s}},$$

for X sufficiently large depending on s .

Finally, the proof of the upper bound for $C_{s,K}(X)$ is the same, now using Lemma 5.4 instead. \square

As a corollary of the previous Lemma, we get Theorem 5.1, by just dividing $C_{s,K}(X)$ by $C_s(X)$.

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. 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 [13] 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.

Acknowledgements. The second author is partially supported by Dusk Network and the Spanish grant PID2019-110224RB-I00.

References

1. SageMath code from Appendix C. GitHub repository (2022), <https://github.com/pairingfriendlycycles/pairing-friendly-cycles/tree/main> 3
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) 17, 19
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) 4

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) 18
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. Bowe, S., Grigg, J., Hopwood, D.: Recursive proof composition without a trusted setup. *Cryptology ePrint Archive* (2019) 2
11. Bünz, B., Chiesa, A., Mishra, P., Spooner, N.: Proof-carrying data from accumulation schemes. *Cryptology ePrint Archive* (2020) 2
12. Cahen, P.J., Chabert, J.L.: What you should know about integer-valued polynomials. *The American Mathematical Monthly* **123**(4), 311–337 (2016) 27
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) 2, 3, 10, 13, 21
14. 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
15. Cox, D.A.: Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication. John Wiley & Sons (1989) 4
16. Crandall, R., Pomerance, C.: Prime numbers: A computational perspective. Springer-Verlag, New York (2001)
17. 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
18. Freeman, D.: Constructing pairing-friendly elliptic curves with embedding degree 10. In: International Algorithmic Number Theory Symposium. pp. 452–465. Springer (2006) 3, 5, 6, 7
19. 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
20. Freeman, D., Scott, M., Teske, E.: A taxonomy of pairing-friendly elliptic curves. *Journal of cryptology* **23**(2), 224–280 (2010) 5
21. 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
22. Gabizon, A., Williamson, Z.J., Ciobotaru, O.: Plonk: Permutations over Lagrange-bases for oecumenical noninteractive arguments of knowledge. *Cryptology ePrint Archive* (2019) 1
23. 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, 8
24. 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
25. 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)
26. 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
27. 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)

28. Koblitz, N.: Elliptic curve implementation of zero-knowledge blobs. *J. Cryptology* **4**(3), 207–213 (1991) 19
29. Lenstra, Jr., H.W.: Factoring integers with elliptic curves. *Ann. of Math. (2)* **126**(3), 649–673 (1987) 20
30. Matthews, K.: The diophantine equation $x^2 - dy^2 = n, d > 0$. *Expositiones Mathematicae* **18**(4), 323–332 (2000)
31. 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
32. Migotti, A.: *Aur theorie der kreisteilungsgleichung*. *B. der Math.-Naturwiss, Classe der Kaiserlichen Akademie der Wissenschaften, Wien* **87**, 7–14 (1883) 11
33. 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) 2, 4, 5, 7
34. Montgomery, H.L., Vaughan, R.C.: The large sieve. *Mathematika* **20**(2), 119–134 (1973) 18
35. 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
36. Pegg, E.J.: Bouniakowsky conjecture. MathWorld—A Wolfram Web Resource, created by Eric W. Weisstein <https://mathworld.wolfram.com/BouniakowskyConjecture.html> 5
37. 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)
38. Silverman, J.H.: *The arithmetic of elliptic curves*, vol. 106. Springer (2009) 4, 7
39. Silverman, J.H., Stange, K.E.: Amicable pairs and aliquot cycles for elliptic curves. *Experimental Mathematics* **20**(3), 329–357 (2011) 2, 9, 10
40. Smart, N.P.: The discrete logarithm problem on elliptic curves of trace one. *JOURNAL OF CRYPTOLOGY* **12**, 193–196 (1999) 2
41. Sutherland, A.V.: Accelerating the CM method. *LMS Journal of Computation and Mathematics* **15**, 172–204 (2012) 5
42. Valiant, P.: Incrementally verifiable computation or proofs of knowledge imply time/space efficiency. In: *Theory of Cryptography Conference*. pp. 1–18. Springer (2008) 1
43. 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

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

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			Bounds for BN		
ℓ	A	B	ℓ	A	B
5	-104	104	3	-1	0
10	-75658	75657	4	-3	4
19	-10626317415	10626317415	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

Bounds for Freeman		
ℓ	A	B
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

Table 2. Bounds A, B 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

C.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:

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

```

1 # SETUP
2
3 # Polynomial rings over the reals and rationals.
4 R.<X> = PolynomialRing(RR, 'X')
5 Q.<X> = PolynomialRing(QQ, 'X')
6
7 # Curve families.
8 def MNT3():
9     t = Q(6*X - 1)
10    q = Q(12*X^2 - 1)
11    p = q + 1 - t
12    return(t, p, q)
13
14 def MNT4():
15    t = Q(-X)
16    q = Q(X^2 + X + 1)
17    p = q + 1 - t
18    return(t, p, q)
19
20 def MNT6():
21    t = Q(2*X + 1)
22    q = Q(4*X^2 + 1)
23    p = q + 1 - t
24    return(t, p, q)
25
26 def Freeman():
27    t = Q(10*X^2 + 5*X + 3)
28    q = Q(25*X^4 + 25*X^3 + 25*X^2 + 10*X + 3)
29    p = q + 1 - t
30    return(t, p, q)
31
32 def BN():
33    t = Q(6*X^2 + 1)
34    q = Q(36*X^4 + 36*X^3 + 24*X^2 + 6*X + 1)
35    p = q + 1 - t
36    return(t, p, q)

```

C.2 Code for Proposition 4.1

`candidate_embedding_degrees(Family, K)`

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: a bound on the embedding degree to look for.

The expected outputs are:

- `embedding_degrees`: a list of potential embedding degrees k such that $3 \leq k \leq K$ and a curve from the family *might* form a cycle with a curve with embedding degree k .
- `modular_conditions`: conditions on $x \bmod k$ for each of these k .

```
1 def candidate_embedding_degrees(Family, K):
2
3     (t, p, q) = Family()
4     # Create an empty list to store the candidate embedding degrees.
5     embedding_degrees = []
6     # Create an empty list to store the lists of modular conditions for
7     # each k.
8     modular_conditions = [None] * (K+1)
9
10    # Embedding degree k implies that q(x) = 1 (mod k).
11    # We check this condition in 0, ..., k-1 and build a list of candidates
12    # such that any x has to be congruent to one of them modulo k.
13    for k in range(3, K+1):
14
15        candidate = False
16
17        for i in range(k):
18            if ((q(i) % k) == 1):
19                # First time a candidate k is discovered, add it to the
20                # list and create a list within modular_conditions to store
21                # the values i.
22                if (not candidate):
23                    candidate = True
24                    embedding_degrees.append(k)
25                    modular_conditions[k] = []
26                    modular_conditions[k].append(i)
27
28    return embedding_degrees, modular_conditions
```

C.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 $x \in \mathbb{Z}$ [12, Corollary 2].

```
1 def is_integer_valued(g):
2
3     # Check if evaluation is integer in deg(g) + 1 consecutive points.
4     for x in range(g.degree()+1):
5         if (not g(x) in ZZ):
6             print(str(g) + " is not integer-valued.")
7             return False
8     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.

```
1 def find_relevant_root(w, b, side):
2
3     # Decide whether to keep the left-most or right-most root.
4     i = -(1 + side) / 2
5
6     # 0 <= w(x)
7     C_1 = 0
8     w_roots = R(w).roots()
9     if (w_roots != []):
10         C_1 = w_roots[i][0]
11
12     # w(x) < b(x)
13     C_2 = 0
14     bw_roots = R(b - w).roots()
15     if (bw_roots != []):
16         C_2 = bw_roots[i][0]
17
18     # Return the relevant extremal root.
19     if (side == -1):
20         return ceil(min(C_1, C_2))
21     else:
22         return floor(max(C_1, C_2))
```

C.4 Code for Table 2

```
compute_bounds(a, b)
```

This function computes the bounds A, B of Lemma 4.4, which has been used to produce the results of tables from Figure 2. It uses the auxiliary functions from Appendix C.3.

The expected inputs are:

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

The expected outputs are:

- **A, B**: integer bounds as described in Lemma 4.4.

```

1 def compute_bounds(a, b):
2     # Check that b has even degree and positive leading coefficient.
3     if (b.degree() % 2 == 1 or b.leading_coefficient() < 0):
4         print("Invalid divisor.")
5         return
6     # Check that a, b are integer valued.
7     if (not is_integer_valued(a) or not is_integer_valued(b)):
8         return
9     # Polynomial division.
10    (h, r) = a.quo_rem(b)
11    # Compute c so that ch, cr are in Z[X].
12    denominators = [i.denominator() for i in (h.coefficients() + r.
13    coefficients())]
14    c = lcm(denominators)
15    # Compute signs.
16    sigma_B = sign(r.leading_coefficient())
17    sigma_A = sigma_B * (-1)^(r.degree())
18    # Compute the polynomials w_A, w_B such that
19    # 0 <= w_A < b(x) for all x < A, and
20    # 0 <= w_B < b(x) for all x > B.
21    w_A = c * r + ((1 - sigma_A) / 2) * b
22    w_B = c * r + ((1 - sigma_B) / 2) * b
23    # Compute A, B.
24    A = find_relevant_root(w_A, b, -1)
25    B = find_relevant_root(w_B, b, 1)
    return (A, B)

```

C.5 Code for Corollary 4.8

`exhaustive_search(Family, k, A, B, mod_cond)`

This function performs the exhaustive search from Corollary 4.8 within the intervals $[A, B]$.

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.
- `A, B`: upper and lower integer bounds.
- `mod_cond`: conditions on $x \bmod k$ for every x in the interval $[A, B]$.

The expected output is:

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

```

1 def exhaustive_search(Family, k, A, B, mod_cond):
2
3     (t, p, q) = Family()
4     curves = []
5
6     for x in range(A, B+1):
7         # We skip those values that will never yield q(x) = 1 (mod k), as
8         # precomputed above.
9         if (not (x % k) in mod_cond): continue
10        # Check the embedding degree condition.
11        if (p(x)^k - 1 % q(x) == 0):
12            curves.append((x, k, t(x), p(x), q(x)))
13
14    return curves

```

C.6 Main function

`search_for_cycles(Family, K)`

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 less than a given bound.

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 integer bound on the embedding degree to look for.

The function prints out all 2-cycles involving a curve from the family and a prime-order curve with embedding degree $k < K$.

```
1 def search_for_cycles(Family, K):
2
3     # Instantiate the family.
4     (t, p, q) = Family()
5     print("Starting family: " + str(Family.__name__))
6     print("t(X) = " + str(t))
7     print("p(X) = " + str(p))
8     print("q(X) = " + str(q))
9
10    # Find the candidate embedding degrees up to K that are compatible with
11    # this family.
12    (embedding_degrees, modular_conditions) = candidate_embedding_degrees(
13    Family, K)
14    print("Candidate embedding degrees: " + str(embedding_degrees))
15    for k in embedding_degrees:
16        print((k, modular_conditions[k]))
17        print("=====")
18
19    # For each potential embedding degree, find the bounds A, B and perform
20    # exhaustive search within [A, B].
21    for k in embedding_degrees:
22
23        print("k = " + str(k))
24        (A, B) = compute_bounds(p^k, q)
25        print("A = " + str(A) + ", B = " + str(B))
26
27        curves = exhaustive_search(Family, k, A, B, modular_conditions[k])
28        print("Curves with embedding degree " + str(k) + " that form a
29        cycle with a curve from the " + str(Family.__name__) + " family: " +
30        str(len(curves)))
31
32        for curve in curves:
33            (x, k, t, p, q) = curve
34            print("x = " + str(x))
35            print("embedding degree = " + str(k))
36            print("t(x) = " + str(t))
37            print("p(x) = " + str(p))
38            print("q(x) = " + str(q))
39            print("-----")
```