



# On pairing-friendly 2-cycles and SNARK-friendly 2-chains of elliptic curves containing a curve from a prime-order family

Tomáš Novotný<sup>1</sup>  and Vladimír Sedláček<sup>2</sup> 

<sup>1</sup> RWTH Aachen University, Aachen, Germany

<sup>2</sup> Masaryk University Brno, Brno, Czech Republic

**Abstract.** Cryptographic protocols such as zk-SNARKs use 2-cycles of elliptic curves for efficiency, often relying on pairing computations. However, 2-cycles of pairing-friendly curves are hard to find, and the only known cases consist of an MNT<sub>4</sub> and an MNT<sub>6</sub> curve. In this work, we prove that a 2-cycle containing an MNT<sub>3</sub>, Freeman, or BN curve cannot be pairing-friendly. Thus we cannot hope to find new pairing-friendly 2-cycles using the current methods.

Furthermore, we show that there are no SNARK-friendly 2-chains of elliptic curves from combinations of MNT, Freeman and BN curves of reasonable size, except for (MNT<sub>4</sub>, MNT<sub>6</sub>).

**Keywords:** Cycles of elliptic curves · chains of elliptic curves · pairing-friendly curves

## 1 Introduction

Pairings of elliptic curves play an important role in the modern zero-knowledge protocols, such as zk-SNARKs. Ben-Sasson et al. [BSCTV14] showed how to use *cycles of pairing-friendly elliptic curves* to provide a scalable implementation. However, this requires 2-cycles of prime-order curves with small and similar embedding degrees, as we need the pairings on the curves to be efficiently computable. The fundamental question is whether it is possible to construct such 2-cycles. We provide a negative answer under various assumptions.<sup>1</sup>

Currently, the only method to find a curve with a prescribed embedding degree is to use *families of curves* [FST10] defined by triples of polynomials that describe the curve parameters. The only known families of prime-order elliptic curves are the MNT [MNT01], Freeman [Fre06], and the Barreto-Naehrig [BN06] families.

The concept of a 2-cycle can also be weakened to a 2-chain, which has applications in zk-SNARKs as well. Finding *SNARK-friendly* 2-chains is in general a hard problem as well.

After some preliminaries (Section 2), we offer three main contributions. We show that

- for an arbitrary family of prime-order curves, the embedding degree of the second curve in the cycle is either constant or grows at least logarithmically with the field size (Theorem 3.3 in Section 3).
- there are no pairing-friendly 2-cycles of prime-order curves containing a curve from one of the three families above, except for (MNT<sub>4</sub>, MNT<sub>6</sub>) cycles (Theorem 3.12 in Section 3).
- there are no cryptographically relevant SNARK-friendly 2-chains of prime-order curves containing a curve from one of the three families above, except for (MNT<sub>4</sub>, MNT<sub>6</sub>) chains (Theorem 4.11 in Section 4).

---

E-mail: [tomas.novotny@rwth-aachen.de](mailto:tomas.novotny@rwth-aachen.de) (Tomáš Novotný), [vlada.sedlacek@mail.muni.cz](mailto:vlada.sedlacek@mail.muni.cz) (Vladimír Sedláček)

<sup>1</sup>A part of this work is based on the bachelor's thesis of the first author [Nov17].



## 2 Preliminaries

In this section, we set the stage with classical results from algebra and number theory [DFo4, Cox13, Was08, GG13], as well as more context about 2-cycles [FST10, CCW19]. Throughout the paper,  $\mathbb{N}$  will denote the set of positive integers.

### 2.1 Cyclotomic polynomials

For  $k \in \mathbb{N}$ , we denote  $\zeta_k := e^{\frac{2\pi i}{k}} \in \mathbb{C}$  and define the  $k$ -th cyclotomic polynomial  $\Phi_k(x)$  as  $\Phi_k(x) := \prod_{\gcd(k,i)=1} (x - \zeta_k^i)$ .

**Lemma 2.1.** *Let  $k \in \mathbb{N}$ . Then  $\Phi_k(x) \in \mathbb{Z}[x]$  and  $x^k - 1 = \prod_{d|k} \Phi_d(x)$ .*

### 2.2 Elliptic curves and 2-cycles

Let  $\mathbb{F}_q$  denote the finite field with  $q$  elements. For any  $a, b \in \mathbb{F}_q$  satisfying  $4a^3 - 27b^2 \neq 0$ , we define an *elliptic curve*  $E/\mathbb{F}_q$  as the set  $E(\mathbb{F}_q) := \{(x, y) \in \mathbb{F}_q^2 \mid y^2 = x^3 + ax + b\} \cup \{\infty\}$ . In this work, we will only consider the cases where both  $q$  and  $|E(\mathbb{F}_q)|$  are distinct odd primes<sup>2</sup>. In that case, the *embedding degree* of  $E/\mathbb{F}_q$  is the smallest  $k \in \mathbb{N}$  such that  $|E(\mathbb{F}_q)|$  divides  $q^k - 1$ . If  $k < \frac{\log_2(q)}{8}$ , we call  $E/\mathbb{F}_q$  *pairing-friendly* [FST10]. This is important for pairing-based cryptography. We also have a characterization using cyclotomic polynomials:

**Lemma 2.2.** [CCW19, Lemma 1.2] *Let  $|E(\mathbb{F}_q)|$  be a prime. Then  $E/\mathbb{F}_q$  has embedding degree  $k$  if and only if  $k$  is minimal such that  $r$  divides  $\Phi_k(q)$ , or equivalently,  $r$  divides  $\Phi_k(q - r)$ .*

A *2-cycle of elliptic curves* is a pair of curves  $E_1/\mathbb{F}_{q_1}, E_2/\mathbb{F}_{q_2}$  such that  $|E_1(\mathbb{F}_{q_1})| = q_2$  and  $|E_2(\mathbb{F}_{q_2})| = q_1$ . We call a 2-cycle of type  $(k_1, k_2)$  if  $k_1, k_2$  are the embedding degrees of  $E_1/\mathbb{F}_{q_1}$  and  $E_2/\mathbb{F}_{q_2}$ , respectively, and pairing-friendly if both its curves are pairing-friendly.

Every elliptic curve  $E/\mathbb{F}_q$  satisfies the classical Hasse bound [Cox13, Theorem 14.12]:

$$q + 1 - 2\sqrt{q} \leq r \leq q + 1 + 2\sqrt{q}, \quad (1)$$

where  $r = |E(\mathbb{F}_q)|$ . In fact, given odd distinct primes  $q, r$  satisfying (1), there exists an elliptic curve<sup>3</sup>  $E/\mathbb{F}_q$  with  $|E(\mathbb{F}_q)| = r$ . Hence, instead of considering 2-cycles of elliptic curves, we can equivalently focus just on pairs  $(q, r)$ . Moreover, it is not difficult to show that  $(q, r)$  satisfies (1) if and only if  $(r, q)$  satisfies it [Nov17, BMUS23].

### 2.3 Families of prime-order curves

To find the parameters  $q, r$  of elliptic curves, we can use *families of prime-order curves of embedding degree  $k$* , which are defined as triplets  $\mathcal{F} = (q(x), r(x), t(x))$  of polynomials with rational coefficients satisfying some formal conditions [FST10, Definition 2.7]. We will require only three conditions which are relevant for our context:

- (i)  $q(x), r(x)$  are integer-valued (i.e., we have  $q(m), r(m) \in \mathbb{Z}$  for all  $m \in \mathbb{Z}$ ),
- (ii)  $r(x) = q(x) + 1 - t(x)$ , and
- (iii)  $r(x) \mid \Phi_k(t(x) - 1)$ .

Miyaji, Nakabayashi, and Takano [MNT01] gave families of prime-order elliptic curves with embedding degrees 3, 4 and 6. In fact, if a prime-order curve over a field of size at least 64 has

<sup>2</sup>This already implies that the curve is not supersingular nor anomalous.

<sup>3</sup>Determined uniquely up to an isogeny.

an embedding degree  $k \in \{3, 4, 6\}$ , then the curve is in the their families, represented by the polynomials

$$\begin{aligned} q_{\text{MNT}_3}(x) &= 12x^2 - 1, & r_{\text{MNT}_3}(x) &= 12x^2 - 6x + 1, & t_{\text{MNT}_3}(x) &= 6x - 1, \\ q_{\text{MNT}_4}(x) &= x^2 + x + 1, & r_{\text{MNT}_4}(x) &= x^2 + 2x + 2, & t_{\text{MNT}_4}(x) &= -x, \\ q'_{\text{MNT}_4}(x) &= x^2 + x + 1, & r'_{\text{MNT}_4}(x) &= x^2 + 1, & t'_{\text{MNT}_4}(x) &= x + 1, \\ q_{\text{MNT}_6}(x) &= 4x^2 + 1, & r_{\text{MNT}_6}(x) &= 4x^2 + 2x + 1, & t_{\text{MNT}_6}(x) &= -2x + 1. \end{aligned}$$

Freeman [Fre06] found another family of prime-order elliptic curves with embedding degree 10, and Barreto and Naehrig used a different technique to obtain a family of prime-order elliptic curves [BN06]. Their families are represented by the polynomials

$$\begin{aligned} q_{\text{FR}}(x) &= 25x^4 + 25x^3 + 25x^2 + 10x + 3, & q_{\text{BN}}(x) &= 36x^4 + 36x^3 + 24x^2 + 6x + 1, \\ r_{\text{FR}}(x) &= 25x^4 + 25x^3 + 15x^2 + 5x + 1, & r_{\text{BN}}(x) &= 36x^4 + 36x^3 + 18x^2 + 6x + 1, \\ t_{\text{FR}}(x) &= 10x^2 + 5x + 3, & t_{\text{BN}}(x) &= 6x^2 + 1. \end{aligned}$$

We denote the MNT3 family as MNT3, the Freeman family as FR and the BN family as BN. We say a cycle is of type  $(\mathcal{F}, k)$  if  $E_1$  is from the family  $\mathcal{F}$  and  $E_2$  has embedding degree  $k$ .

## 2.4 Auxiliary results

We will also need the following adaptation of long division of polynomials.

**Lemma 2.3** (Pseudo division [GG13, Section 6.12]). *Let  $p(x), q(x) \in \mathbb{Z}[x]$  be two polynomials with integer coefficients, let  $q_n$  be the leading coefficient of  $q(x)$  and let  $n = \deg q(x)$ . Then there are unique polynomials  $f(x), r(x) \in \mathbb{Z}[x]$  with  $\deg r(x) < \deg q(x)$  and*

$$q_n^{n+1}p(x) = f(x)q(x) + r(x). \quad (2)$$

**Lemma 2.4** (Generalized Pell equation, [Con17]). *Let  $d$  be a positive non-square integer, and let  $a, b \in \mathbb{N}$  such that  $a^2 - db^2 = 1$ . For every  $n \in \mathbb{Z} \setminus \{0\}$ , every integral solution  $(r, s)$  of  $x^2 - dy^2 = n$  is of the form*

$$r + s\sqrt{d} = (x' + y'\sqrt{d}) \cdot (a + b\sqrt{d})^k$$

for some  $k \in \mathbb{Z}$  and some  $x', y' \in \mathbb{Z}$  such that  $x'^2 - dy'^2 = n$ , and

$$|x'| \leq \frac{\sqrt{|n|}(\sqrt{u} + 1/\sqrt{u})}{2} \quad \text{and} \quad |y'| \leq \frac{\sqrt{|n|}(\sqrt{u} + 1/\sqrt{u})}{2\sqrt{d}}. \quad (3)$$

## 3 Cycles containing a curve from a prime-order family

**Definition 3.1.** Let  $\mathcal{F} = (q(x), r(x), t(x))$  be a family representing prime-order elliptic curves and let  $k \in \mathbb{N}$ . We call  $\mathcal{F}$  *cycle-friendly with  $k$* , if  $k$  is minimal such that  $q(x)$  divides  $\Phi_k(1 - t(x))$  in  $\mathbb{Z}[x]$ . If there exist such  $k$ , we call  $\mathcal{F}$  *cycle-friendly*. Otherwise, we call  $\mathcal{F}$  *cycle-unfriendly*.

**Example 3.2.** The MNT4 and MNT6 families are cycle-friendly with 6 and 4, respectively. In Theorem 3.6, we will show that MNT3, FR, and BN are cycle-unfriendly.

The main result of this section is the following theorem:

**Theorem 3.3.** *Let  $\mathcal{F}$  be a family of prime-order elliptic curves.*

- (a) If  $\mathcal{F}$  is cycle-friendly with  $k$ , then all but finitely many curves in the family  $\mathcal{F}$  form an  $(\mathcal{F}, k)$ -cycle, or
- (b) If  $\mathcal{F}$  is cycle-unfriendly, then any  $k \in \mathbb{N}$  and any 2-cycle of type  $(\mathcal{F}, k)$  has to satisfy  $k \in \Omega(\log r)$ , where  $r$  is the field size of the second curve in the cycle, and the implied constant depend only on the family  $\mathcal{F}$ .

We will prove both cases<sup>4</sup> in Section 3.1 and Section 3.2, respectively.

*Remark 3.4.* In [Nov17], we proved that if a family  $\mathcal{F}$  is cycle-unfriendly, then for any  $k$ , there are only finitely many  $(\mathcal{F}, k)$ -cycles. (Later, Bellés–Muñoz et al. showed a similar statement [BMUS23, Theorem 4.5].) Case (b) of Theorem 3.3 is a much stronger result.

Furthermore, if  $\mathcal{F}$  is cycle-unfriendly, both [Nov17] and [BMUS23] computationally find the cycles of type  $(\mathcal{F}, k)$  for MNT3, Freeman, and BN families and  $k \leq 22$  and find that none of them are of cryptographic interest. This answered the question of [CCW19] whether there are 2-cycles of combinations of the known prime-order families.

### 3.1 Cycle-friendly families

*Proof of case (a) of Theorem 3.3.* Let  $\mathcal{F} = (q(x), r(x), t(x))$  be a family representing prime-order elliptic curves that is cycle-friendly with  $k$ . By definition,  $q(x)$  divides  $\Phi_k(1 - t(x))$  in  $\mathbb{Z}[x]$ . Let  $m \in \mathbb{Z}$  such that there is a curve  $E_1$  with field size  $q(m)$  and size  $r(m)$ , and a curve  $E_2$  with field size  $r(m)$  and size  $q(m)$ .

Since both  $q(x)$  and  $\Phi_k(1 - t(x))$  are integer-valued, we have that for any  $m \in \mathbb{Z}$ ,

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

and hence, by Theorem 2.2, the embedding degree of  $E_2$  is at most  $k$ . We will show that it can be strictly less than  $k$  only in finitely many values of  $m$ .

By definition of cycle-friendliness, for any  $k' < k$ , the polynomial  $q(x)$  does not divide  $\Phi_{k'}(1 - t(x))$ . By Theorem 2.3, we can write

$$l \cdot \Phi_{k'}(1 - t(x)) = q(x)g(x) + r(x)$$

for  $g(x), r(x) \in \mathbb{Z}[x]$ ,  $\deg r(x) < \deg q(x)$  and  $r(x)$  is not constant zero. We see that for any  $m \in \mathbb{Z}$ ,

$$q(m) \mid \Phi_{k'}(1 - t(m)) \implies q(m) \mid l \cdot \Phi_{k'}(1 - t(m)) \implies q(m) \mid r(m),$$

since both  $q(x)$  and  $g(x)$  are integer-valued. Since  $\deg r(x) < \deg q(x)$ , for sufficiently large  $M \in \mathbb{Z}$  it holds that  $|r(i)| < |q(i)|$  for any  $i$  for which  $|i| > |M|$ . It follows that all  $m \in \mathbb{Z}$  such that  $q(m) \mid \Phi_{k'}(1 - t(m))$  satisfy  $|m| < |M|$  and hence there are only finitely many  $(\mathcal{F}, k')$ -cycles. Therefore, for any  $k' < k$ , there are at most finitely many  $(\mathcal{F}, k')$ -cycles, implying that all but finitely many curves from  $\mathcal{F}$  form a  $(\mathcal{F}, k)$ -cycle.  $\square$

We also showed in [Nov17] that the MNT3, FR, and BN families are cycle-unfriendly. This is an easy corollary of the following lemma.

**Lemma 3.5.** [Fre06, Lemma 5.1] *Let  $f(x) \in \mathbb{Q}[x]$ ,  $k$  be a positive integer and  $r(x)$  be an irreducible factor (over  $\mathbb{Q}$ ) of  $\Phi_k(f(x))$ . Then  $\varphi(k) \mid \deg r(x)$ , where  $\varphi$  is the Euler totient function.*

**Corollary 3.6.** *The families MNT3, FR, BN are cycle-unfriendly.*

*Proof.* Suppose that the family  $\mathcal{F} \in \{\text{MNT3}, \text{FR}, \text{BN}\}$  is cycle-friendly with some  $k$ . By definition,  $q_{\mathcal{F}}(x)$  is irreducible, and hence Lemma 3.5 implies that  $\varphi(k) \mid \deg q_{\mathcal{F}}(x) \leq 4$ . However,  $\varphi(k) \mid 4$  only for  $k \leq 12$ , and then it is easy to check, for all such  $k$ 's, that  $q_{\mathcal{F}}(x)$  does not divide  $\Phi_k(1 - t_{\mathcal{F}}(x))$  in  $\mathbb{Z}[x]$ .  $\square$

<sup>4</sup>We remark that the conclusions in the two cases are not necessarily exclusive; it is only conjectural that a family of elliptic curves, as defined, gives rise to infinitely many prime-order curves.

### 3.2 Cycle-unfriendly families

We now proceed to study the cycle-unfriendly case more carefully. Namely, for any family  $\mathcal{F}$  and  $k \in \mathbb{N}$ , we can find the bound  $2^{O(k)}$  on the field size of the curves in any  $(\mathcal{F}, k)$ -cycle (where the implied constant depends only on the family  $\mathcal{F}$ ), proving the second part of Theorem 3.3. In Section 3.3, we then compute the constant explicitly for the MNT3, FR, and BN families and prove Theorem 3.12.

**Definition 3.7.** Let  $z_1, \dots, z_n \in \mathbb{C}$ . We define

$$Z(z_1, \dots, z_n) := \max\{|z_i| \mid |z_i| \geq 2\} \cup \{|z_i| + 1 \mid |z_i| < 2\}$$

**Lemma 3.8.** Let  $k \geq 1$  and  $z_1, \dots, z_n \in \mathbb{C}$ . Then

$$\max_i |\Phi_k(z_i)| \leq Z(z_1, \dots, z_n)^k + 1$$

*Proof.* For a fixed  $i \in \{1, \dots, n\}$ , we have two options:

1.  $|z_i| < 2$ . Then

$$|\Phi_k(z_i)| = \prod_{(j,k)=1} |z_i - \zeta_k^j| \leq \prod_{(j,k)=1} |z_i| + |\zeta_k^j| = (|z_i| + 1)^{\varphi(k)} < (|z_i| + 1)^k + 1.$$

2.  $|z_i| \geq 2$ . Then for any  $j \in \{1, \dots, n\}$ , we have  $|z_i - \zeta_k^j| \geq |z_i| - |\zeta_k^j| \geq 1$ , so that

$$|\Phi_k(z_i)| = \frac{|z_i^k - 1|}{\prod_{d|k, d < k} |\Phi_d(z_i)|} \leq \frac{|z_i^k - 1|}{\prod_{d|k, d < k} \prod_{(j,d)=1} |z_i - \zeta_d^{j \frac{k}{d}}|} \leq |z_i^k - 1| \leq |z_i|^k + 1,$$

where the first equality comes from Theorem 2.1.

The statement now follows from Definition 3.7.  $\square$

**Lemma 3.9.** Let  $q(x) \in \mathbb{Q}[x]$  be a polynomial of degree  $n$  with distinct complex roots  $\alpha_1, \dots, \alpha_n$ . There is a constant  $c_1 \in \mathbb{R}_+$  (depending only on  $q(x)$ ) such that for any  $k \in \mathbb{N}$  and any polynomial  $f(x)$ , there are  $R_{k,i} \in \mathbb{Q}$  for  $0 \leq i \leq n-1$  and a polynomial  $g(x)$  such that

$$\Phi_k(f(x)) = g(x)q(x) + R_{k,n-1}x^{n-1} + \dots + R_{k,0}, \quad (4)$$

and  $|R_{k,i}| \leq c_1 \cdot Z(f(\alpha_1), \dots, f(\alpha_n))^k$  for all  $i \in \{0, \dots, n-1\}$ .

*Proof.* The existence of  $g(x)$  and the  $R_{k,i}$ 's holds by long division of polynomials. By plugging in  $\alpha_1, \dots, \alpha_n$  in (4), we obtain a linear system of  $n$  equations in variables  $R_{k,0}, \dots, R_{k,n-1}$ :

$$\Phi_k(f(\alpha_i)) = R_{k,n-1}\alpha_i^{n-1} + \dots + R_{k,1}\alpha_i + R_{k,0}$$

We rewrite this as matrix multiplication:

$$\begin{bmatrix} \alpha_1^{n-1} & \dots & \alpha_1 & 1 \\ \alpha_2^{n-1} & \dots & \alpha_2 & 1 \\ \vdots & \ddots & \vdots & \vdots \\ \alpha_n^{n-1} & \dots & \alpha_n & 1 \end{bmatrix} \begin{bmatrix} R_{k,n-1} \\ R_{k,n-2} \\ \vdots \\ R_{k,0} \end{bmatrix} = \begin{bmatrix} \Phi_k(f(\alpha_1)) \\ \Phi_k(f(\alpha_2)) \\ \vdots \\ \Phi_k(f(\alpha_n)) \end{bmatrix}$$

Denote the matrix of coefficients as  $V$ . Since  $V$  is a Vandermonde matrix and all complex roots of  $q(x)$  are distinct,  $V$  is invertible [HJ12], so we can multiply both sides by  $V^{-1}$ :

$$\begin{bmatrix} R_{k,n-1} \\ R_{k,n-2} \\ \vdots \\ R_{k,0} \end{bmatrix} = V^{-1} \begin{bmatrix} \Phi_k(f(\alpha_1)) \\ \Phi_k(f(\alpha_2)) \\ \vdots \\ \Phi_k(f(\alpha_n)) \end{bmatrix}.$$

Applying absolute value and triangle inequality yields

$$|R_{k,i}| \leq \sum_{1 \leq j \leq n} |(V^{-1})_{ij}| \cdot |\Phi_k(f(\alpha_j))| \leq n \cdot \max_j |(V^{-1})_{ij}| \cdot \max_j |\Phi_k(f(\alpha_j))|.$$

Note that  $c := \max_{i,j} |(V^{-1})_{ij}|$  is a constant depending only on  $q(x)$  and let  $c_1 := 2cn$ . Then

$$|R_{k,i}| \leq cn \cdot \max_j |\Phi_k(f(\alpha_j))| \leq cn \cdot Z(f(\alpha_1), \dots, f(\alpha_n))^k + cn \leq c_1 \cdot Z(f(\alpha_1), \dots, f(\alpha_n))^k$$

by Lemma 3.8, and by the observation that  $Z(f(\alpha_1), \dots, f(\alpha_n)) \geq 1$ .  $\square$

**Lemma 3.10.** *Let  $q(x) \in \mathbb{Q}[x]$  be an integer valued polynomial of degree  $n$  with distinct non-zero complex roots  $\alpha_1, \dots, \alpha_n$ . Let  $f(x)$  be a polynomial and  $k \in \mathbb{N}$  such that  $q(x)$  does not divide  $\Phi_k(f(x))$  as polynomials. Then for any  $m \in \mathbb{Z}$  such that  $q(m)$  divides  $\Phi_k(f(m))$  in  $\mathbb{Z}$ , we have*

$$|m| \leq c_2 \cdot Z(f(\alpha_1), \dots, f(\alpha_n))^k \in 2^{O(k)}, \text{ and} \quad (5)$$

$$k \geq \frac{\log_2 |q(m)|}{n \cdot \log_2 Z(f(\alpha_1), \dots, f(\alpha_n))} - c_3 \in \Omega(\log |q(m)|). \quad (6)$$

where both  $c_2, c_3 > 0$  depend only on  $q(x)$ . The implied constants depend only on  $q(x)$  and  $f(x)$ .

*Proof.* Let  $q_n$  be the leading coefficient of  $q(x)$  and let  $l \in \mathbb{Z}$  be the smallest integers such that we can write

$$l \cdot \Phi_k(f(x)) = g(x)q(x) + r(x) \quad (7)$$

where  $g(x), r(x) \in \mathbb{Z}[x]$  and  $\deg r(x) < \deg q(x)$ . By Theorem 2.3, we know that  $l \leq q_n^{n+1}$ .

By the uniqueness of long division, we have

$$r(x) = l \cdot R_{k,n-1}x^{n-1} + \dots + l \cdot R_{k,0}$$

for numbers  $R_{k,i}$ ,  $i \in [n-1]$ , given by Theorem 3.9. Note that  $r(x)$  is not a constant zero, since  $q(x)$  does not divide  $\Phi_k(f(x))$  as polynomials.

Let  $m \in \mathbb{Z}$  be such that  $q(m) \in \mathbb{Z}_{\neq 0}$  divides  $\Phi_k(f(m)) \in \mathbb{Z}$ . If  $m = 0$ , then the lemma holds trivially. Hence suppose  $m \neq 0$ . Since both  $q(x)$  and  $g(x)$  are integer valued, we have

$$q(m) \mid \Phi_k(f(m)) \implies q(m) \mid l \cdot R_{k,n-1}m^{n-1} + \dots + l \cdot R_{k,0} \quad \text{by 7.}$$

In particular, we have

$$\begin{aligned} |q(m)| &\leq l \cdot |R_{k,n-1}m^{n-1} + \dots + R_{k,0}| \\ &\leq l \cdot |R_{k,n-1}m^{n-1}| + \dots + l \cdot |R_{k,1}m| + l \cdot |R_{k,0}| \quad \text{by triangle inequality} \\ &\leq l \cdot |m|^{n-1} \cdot \sum_{i=1}^{n-1} |R_{k,i}|. \end{aligned} \quad (8)$$

After dividing this inequality by  $|m|^{n-1}$ , we get

$$\left| \frac{q(m)}{m^{n-1}} \right| \leq \sum_{i=0}^{n-1} l \cdot |R_{k,i}| \leq l \cdot n \cdot c_1 \cdot Z(f(\alpha_1), \dots, f(\alpha_n))^k$$

by Lemma 3.9. Let  $Z := Z(f(\alpha_1), \dots, f(\alpha_n))$ . Now suppose that  $q(x) = \sum_{0 \leq i \leq n} q_i x^i$  for some  $q_1, \dots, q_n \in \mathbb{Q}$  with  $q_n \neq 0$ . Then

$$|q_n| \cdot |m| - \sum_{i=0}^{n-1} |q_i| \leq |q_n| \cdot |m| - \sum_{i=0}^{n-1} |q_i m^{i-n+1}| \leq \left| q_n m + \sum_{i=0}^{n-1} q_i m^{i-n+1} \right| = \left| \frac{q(m)}{m^{n-1}} \right|,$$

hence

$$|m| \leq |q_n|^{-1} \left( l \cdot n \cdot c_1 \cdot Z^k + \sum_{i=0}^{n-1} |q_i| \right).$$

Define  $c_2 := \frac{1}{|q_n|} \left( l \cdot n \cdot c_1 + \sum_{i=0}^{n-1} |q_i| \right)$ . We have

$$\begin{aligned} |m| &\leq \frac{1}{|q_n|} \left( l \cdot n \cdot c_1 \cdot Z^k + \sum_{i=0}^{n-1} |q_i| \right) \\ &\leq |q_n|^{-1} \left( l \cdot n \cdot c_1 + \sum_{i=0}^{n-1} |q_i| \right) Z^k && \text{since } Z \geq 1 \\ &= c_2 Z^k. \end{aligned}$$

The asymptotic bound in (5) follows from the definition of  $Z$ .

It remains to prove (6). For this, note that by (8),

$$\begin{aligned} |q(m)| &\leq |m^{n-1}| \cdot \sum_{i=1}^{n-1} |R_{k,i}| \\ &\leq c_2^{n-1} Z^{(n-1)k} \cdot nc_1 Z^k && \text{by Theorem 3.9} \\ &= nc_1 c_2^{n-1} \cdot Z^{nk}. \end{aligned}$$

Taking logarithms, we obtain

$$\log_2 k \geq \frac{\log_2 |q(m)|}{n \log_2 Z} - \frac{\log_2 (nc_1 c_2^{n-1})}{n \log_2 Z} = \frac{\log_2 |q(m)|}{n \log_2 Z} - c_3$$

$$\text{for } c_3 = \frac{\log_2 (nc_1 c_2^{n-1})}{n \log_2 Z}.$$

□

*Proof of Theorem 3.3.* The proof for the cycle-friendly case was discussed in Section 3.1.

Let  $\mathcal{F}$  be a prime-order family of elliptic curves such that  $\mathcal{F}$  is cycle-unfriendly. Then  $q_{\mathcal{F}}(x)$  does not divide  $\Phi_k(1 - t_{\mathcal{F}}(x))$  as polynomials for any  $k$ .

Let  $q(x) := q_{\mathcal{F}}(x)$  and  $f(x) := 1 - t_{\mathcal{F}}(x)$ . Note that both  $q(x)$  and  $f(x)$  are integer-valued. Let  $m \in \mathbb{Z}$  be such that the curve specified by  $q(m), r(m)$  is in a  $(\mathcal{F}, k)$ -cycle. Then  $q(m)$  divides  $\Phi_k(f(m))$  and hence by Theorem 3.10,  $k \in \Omega(\log |q(m)|)$ . However, by the Hasse bound, we also have  $k \in \Omega(\log |r(m)|) = \Omega(\log r)$ , where the implied constant depends only on  $q(x)$  and  $f(x)$ , and hence only on the family  $\mathcal{F}$ . □

### 3.3 Exact lower bounds in the known families

Note that from the proofs of Theorem 3.9 and Theorem 3.10, we can compute the constants  $c_3$  and  $n \log_2 Z$  for the MNT3, Freeman, and BN families explicitly and state the following result.

**Proposition 3.11.** *Let  $\mathcal{F} \in \{\text{MNT3}, \text{FR}, \text{BN}\}$ . Suppose that there is a  $(\mathcal{F}, k)$ -cycle where the field size of the first curve is  $q$ .*

- If  $\mathcal{F} = \text{MNT3}$ , then  $k > \frac{\log_2 q(m)}{3.800} - 2.942$ .
- If  $\mathcal{F} = \text{FR}$ , then  $k > \frac{\log_2 q(m)}{7.195} - 9.655$ .
- If  $\mathcal{F} = \text{BN}$ , then  $k > \frac{\log_2 q(m)}{4.798} - 16.435$ .

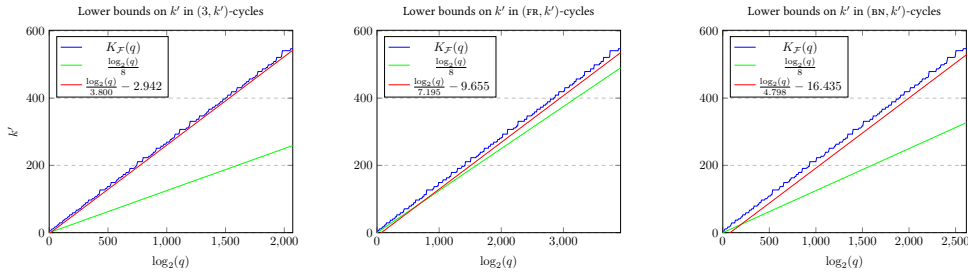


Let  $\mathcal{F}$  be a prime-order family. For any  $k \in \mathbb{N}$ , we define  $Q_{\mathcal{F}}(k)$  as the largest  $|q(m)|$  such that  $|q(m)| \leq l \cdot |R_{k,n-1}m^{n-1} + \dots + R_{k,0}|$  as in Theorem 3.10. Given  $q \in \mathbb{N}$ , we define  $K_{\mathcal{F}}(q)$  to be the smallest  $k$  such that  $Q_{\mathcal{F}}(k) \geq q$ .

Note that we can compute the value  $Q_{\mathcal{F}}(k)$  as follows: for any  $k$ , compute the coefficients  $R_{k,n-1}, \dots, R_{k,0}$ . It turns out that in our computation, it suffices to take  $l = 1$ . Note that any  $m$  satisfies  $|q_{\mathcal{F}}(m)| \leq l \cdot |R_{k,n-1}m^{n-1} + \dots + R_{k,0}|$  if and only if it is a real root of  $q(x)^2 - (R_{k,n-1}x^{n-1} + \dots + R_{k,0})^2$ . Therefore, we compute the real root  $M_k$  of this polynomial that is largest in absolute value (take the positive one, if it is not unique). The value  $Q_{\mathcal{F}}(k)$  can be set to  $q_{\mathcal{F}}(M_k)$ .

We computed the lower bounds  $K_{\mathcal{F}}(q)$  for our families (MNT3, FR, BN) up to the highest  $q$  such that  $K_{\mathcal{F}}(q) \leq 550$ ; so as the computation finishes in reasonable time. Our theoretical bounds seem to match with the computation, as shown in Figure 1.

We can easily check that for all three bounds mentioned in Theorem 3.11, the bound on the embedding degree exceeds  $\frac{\log_2 q}{8}$  when  $q(m) \geq 2^{691}$ . We computationally checked that  $K_{\mathcal{F}}(q) > \frac{\log_2 q}{8}$  for all  $q(m) \leq 2^{691}$ , which concludes the proof of Theorem 3.12.



**Figure 1:** The functions  $K_{\mathcal{F}}(q)$  for  $\mathcal{F} \in \{\text{MNT3}, \text{FR}, \text{BN}\}$ .

**Corollary 3.12.** *There are no pairing-friendly 2-cycles of elliptic curves which contain an MNT3, Freeman, or BN curve.*

## 4 Chains of curves from prime-order families

Recent research [EHG22] also considers weakening the notion of cycles to just *chains*. The idea is that usually we do not need the proof composition to continue forever, but it can stop after some number of recursive calls.

**Definition 4.1.** (Definition 1. in [EHG22]) A 2-chain of prime-order elliptic curves is a pair of curves  $E_1/\mathbb{F}_{q_1}, E_2/\mathbb{F}_{q_2}$ , where  $q_1 \neq q_2$  are primes and  $q_1 = |E_2(\mathbb{F}_{q_2})|$ . The curve  $E_1$  is called the *inner* curve, and  $E_2$  is called the *outer* curve.

Just like for 2-cycles, we say that a 2-chain is of type  $(k_1, k_2)$  if  $k_1, k_2$  are the embedding degrees of  $E_1$  and  $E_2$ , respectively. Analogously, if  $E_1$  and  $E_2$  belong to families  $\mathcal{F}, \mathcal{F}'$ , respectively, we say the 2-chain is of type  $(\mathcal{F}, \mathcal{F}')$ .

The authors of [EHG22] mention that we typically need that all curves in the chain are pairing-friendly and that they have a highly 2-adic subgroup, that is,  $2^L$  divides both  $|E_1(\mathbb{F}_{q_1})| - 1$  and  $|E_2(\mathbb{F}_{q_2})|$  for a large  $L \in \mathbb{N}$ . We will follow their definition and call such chains *SNARK-friendly*. In fact, for our purposes, we can use a very mild definition with  $L \geq 2$ .

We can view a 2-chain as a triple of primes  $(q_1, q_2, q_3)$ , which represents a curve over  $\mathbb{F}_{q_2}$  of order  $q_1$  and another curve over  $\mathbb{F}_{q_3}$  of order  $q_2$ .

In this section, our main goal is to characterise SNARK-friendly 2-chains where both curves are from (possibly different) families of prime-order elliptic curves. We will prove Theorem 4.11.



We will divide the proof into various lemmas and propositions based on the arguments used, as illustrated in Table 1.

**Table 1:** Arguments used to prove that there are no reasonably large 2-chains of elliptic curves in the given families. The abbreviations “mod” means a modulo argument (Section 4.1), “sq” is a squaring argument (Section 4.2), “ineq” is a strategy using inequalities (Section 4.3), “brute” uses the Pell equation together with brute force computations (Section 4.4), and “2-ad” uses the 2-adicity condition (Section 4.5). Note that MNT4–MNT6 cells are left blank as there such chains (even cycles) exist [KTo8].

Inner \ Outer	MNT3	MNT4	MNT6	FR	BN
MNT3	mod	mod	mod	2-ad	mod
MNT4	brute	sq		sq	sq
MNT6	brute		sq	sq	sq
FR	mod	mod	sq	mod	mod
BN	ineq	sq	sq	ineq	ineq

#### 4.1 Modulo argument

A very simple strategy to rule out some 2-chains is to look at the equations modulo some well chosen number.

**Lemma 4.2.** *There are no 2-chains of the following types:*

$$\begin{array}{llll}
 (MNT3, MNT3), & (MNT3, MNT4), & (MNT3, MNT6), & (MNT3, BN) \\
 (FR, MNT3), & (FR, MNT4), & (FR, FR), & (FR, BN)
 \end{array}$$

*Proof.* For any type  $(\mathcal{F}, \mathcal{F}')$  stated in the assertion of the lemma, suppose that there is a 2-chain of that type. Then there must exist some  $a, b \in \mathbb{Z}$  such that  $q_{\mathcal{F}}(a) = r_{\mathcal{F}'}(b)$ . For types  $(MNT3, MNT3)$ ,  $(MNT3, MNT6)$ , and  $(MNT3, BN)$ , we reduce this equation modulo 3. In two of the cases we get an immediate contradiction, and in the case of  $(MNT3, MNT6)$ , we have to argue that  $r_{MNT6}(b) = 4b^2 + 2b + 1$  can only be 0 or 1 modulo 3, while  $q_{MNT3}(a) = 12a^2 - 1$  can only be 2 modulo 3, which is a contradiction.

With a similar strategy, we can prove that there are no cycles of  $(MNT3, MNT4)$  or  $(FR, BN)$ , namely by reducing the equation modulo 4. The rest of the cases can be ruled out by reducing the equation modulo 5.  $\square$

#### 4.2 Squaring argument

**Lemma 4.3.** *There are no 2-chains of the following types:*

$$\begin{array}{lll}
 (MNT4, MNT4), & (MNT4, FR), & (MNT4, BN), \\
 & (MNT6, MNT6), & (MNT6, FR), & (MNT6, BN), \\
 & (FR, MNT6), & \\
 (BN, MNT4), & (BN, MNT6), &
 \end{array}$$

*except for the chain specified by primes (17, 13, 19) of type  $(MNT4, BN)$ .*

*Proof.* For any type  $(\mathcal{F}, \mathcal{F}')$  stated in the assertion of the lemma, suppose that there is a 2-chain of that type. Then there must exist some  $a, b \in \mathbb{Z}$  such that  $q_{\mathcal{F}}(a) = r_{\mathcal{F}'}(b)$ . We can always assume that  $a, b \neq 0$ , since for any of the mentioned families, at least one of  $q_{\mathcal{F}}(0), r_{\mathcal{F}'}(0)$  is not a prime number. The general strategy here is to transform the equation such that one side is a perfect square, and then proving that the other side cannot be a perfect square.

- (MNT<sub>4</sub>, MNT<sub>4</sub>). We must have  $a^2 + a + 1 = q_{\text{MNT}_4}(a) = r'_{\text{MNT}_4}(b) = b^2 + 1$  or  $a^2 + a + 1 = q_{\text{MNT}_4}(a) = r_{\text{MNT}_4}(b) = b^2 + 2b + 2$ . In either way,  $a^2 + a$  must be a perfect square, which implies  $a \in \{-1, 0\}$ , but then  $q_{\text{MNT}_4}(a) = 1$  is not a prime number.
- (MNT<sub>4</sub>, FR). Assume  $q_{\text{MNT}_4}(a) = r_{\text{FR}}(b)$ . Multiplying both sides by 4 and subtracting 3 makes the left-hand side a perfect square, and we obtain that

$$(2a + 1)^2 = 100b^4 + 100b^3 + 60b^2 + 20b + 1 =: K(b).$$

Hence, we need that  $K(b)$  is a perfect square. However, it is easy to show that for all  $b \neq 0$ ,

$$(10b^2 + 5b + 1)^2 < K(b) < (10b^2 + 5b + 2)^2,$$

which implies that  $K(b)$  can never be a perfect square.

- (MNT<sub>4</sub>, BN). Assume  $q_{\text{MNT}_4}(a) = r_{\text{BN}}(b)$ . Multiplying both sides by 4 and subtracting 3 makes the left-hand side a perfect square, and we obtain that

$$(2a + 1)^2 = 144b^4 + 144b^3 + 72b^2 + 24b + 1 =: K(b).$$

It is easy to show that for all  $b \notin \{-1, 0\}$ ,

$$(12b^2 + 6b + 1)^2 < K(b) < (12b^2 + 6b + 2)^2,$$

which implies that  $K(b)$  cannot be a perfect square, unless  $b \in \{0, -1\}$ . The value  $b = -1$  gives rise to the chain specified by the primes (17, 13, 19).

- (MNT<sub>6</sub>, MNT<sub>6</sub>). We must have  $4a^2 + 1 = q_{\text{MNT}_6}(a) = r_{\text{MNT}_6}(b) = 4b^2 + 4b + 1 = (2b + 1)^2$  and hence  $4a^2 + 1$  must be a perfect square, which is impossible for  $a \neq 0$ .
- (MNT<sub>6</sub>, FR). Assume  $q_{\text{MNT}_6}(a) = r_{\text{FR}}(b)$ . Multiplying both sides by 4 and subtracting 4 makes the left-hand side a perfect square, and we obtain that

$$16a^2 = 100b^4 + 100b^3 + 60b^2 + 20b =: K(b).$$

It is again easy to show that for all  $b \neq 0$ ,

$$(10b^2 + 5b + 1)^2 < K(b) < (10b^2 + 5b + 2)^2,$$

which implies that  $K(b)$  cannot be a perfect square for  $b \neq 0$ .

- (MNT<sub>6</sub>, BN). Assume  $q_{\text{MNT}_6}(a) = r_{\text{BN}}(b)$ . We just need that  $r_{\text{BN}}(b) - 1$  is a perfect square. It only suffices to see that for all  $b \neq 0$ ,

$$(6b^2 + 3b)^2 < r_{\text{BN}}(b) - 1 < (6b^2 + 3b + 1)^2,$$

which implies that  $r_{\text{BN}}(b) - 1$  can never be a perfect square.

- (FR, MNT<sub>6</sub>). Assume  $q_{\text{FR}}(a) = r_{\text{MNT}_6}(b)$ . We can multiply both sides by 4, subtract 3 and we obtain that

$$K(a) := 100a^4 + 100a^3 + 100a^2 + 40a + 9 = (4b + 1)^2.$$

It is easy to show that for all  $a \neq 0$ ,

$$(10a^2 + 5a + 3)^2 < K(a) < (12a^2 + 6a + 3)^2,$$

which implies that  $K(a)$  cannot be a perfect square.

- (BN, MNT4). Assume  $q_{\text{BN}}(a) = r'_{\text{MNT4}}(b) = b^2 + 1$  or  $q_{\text{BN}}(a) = r_{\text{MNT4}}(b) = b^2 + 2b + 2$ . In both cases, we need that  $q_{\text{BN}}(a) - 1$  is a perfect square. However, for all  $a \neq 0$ ,

$$(6a^2 + 3a + 1)^2 < q_{\text{BN}}(a) - 1 < (6a^2 + 3a + 2)^2,$$

which implies that  $q_{\text{BN}}(a) - 1$  can never be a perfect square.

- (BN, MNT6). Suppose  $q_{\text{BN}}(a) = r_{\text{MNT6}}(b)$ . We can multiply both sides by 4, subtract 3 and we obtain that

$$K(a) := 144a^4 + 144a^3 + 96a^2 + 24a + 1 = (4b + 1)^2.$$

It is easy to show that for all  $a \neq 0$ ,

$$(12a^2 + 6a + 2)^2 < K(a) < (12a^2 + 6a + 3)^2,$$

which implies that  $K(a)$  cannot be a perfect square.

□

### 4.3 Inequality argument

**Lemma 4.4.** *There are no 2-chains of type (BN, BN).*

*Proof.* Suppose that  $q_{\text{BN}}(a) = r_{\text{BN}}(b)$ . Clearly,  $a, b \neq 0$ .

- Assume  $a, b > 0$ . Since  $r_{\text{BN}}(a) < q(a) = r_{\text{BN}}(b)$  and  $r_{\text{BN}}(a)$  is increasing on  $a \geq 0$ , we can write  $b = a + d$  for some  $d \geq 1$ . But since  $r_{\text{BN}}(a + d) = r_{\text{BN}}(b) = q(a) = r_{\text{BN}}(a) + 6a^2$ , we have

$$6a^2 = r_{\text{BN}}(a + d) - r_{\text{BN}}(a) > r_{\text{BN}}(a + 1) - r_{\text{BN}}(a) = 144a^3 + 324a^2 + 300a + 96,$$

where we again use the monotonicity of  $r_{\text{BN}}(a)$ . But  $144a^3 + 318a^2 + 300a + 96 < 0$  cannot be satisfied for  $a \geq 0$ .

- Now, assume  $a > 0, b < 0$ . Because  $r_{\text{BN}}(-a) < r_{\text{BN}}(a)$  for all  $a > 0$ , we know that  $a < -b$  and hence we can write  $-b = a + d$  for some positive  $d$ . Hence

$$6a^2 = r_{\text{BN}}(-(a + d)) - r_{\text{BN}}(a) > r_{\text{BN}}(-(a + 1)) - r_{\text{BN}}(a) = 72a^3 + 108a^2 + 60a + 12,$$

again contradicting  $a \geq 0$ .

- If  $a < 0, b > 0$ . We want to prove that  $b > -a$ . Suppose there are  $a, b$  such that  $r_{\text{BN}}(a) \leq r_{\text{BN}}(b)$  and  $-a \geq b + 1$ . Then  $r_{\text{BN}}(a) \leq r_{\text{BN}}(b) \leq r_{\text{BN}}(-a - 1)$ , because  $r_{\text{BN}}(a)$  is increasing on the positives. Therefore,

$$72a^3 + 108a^2 + 60a + 12 = r_{\text{BN}}(-a - 1) - r_{\text{BN}}(a) \geq 0,$$

which contradicts the condition  $a \leq 1$ .

Therefore, we have  $b > -a$  and hence a positive  $d$  such that  $b = -a + d$ . Then

$$6a^2 = r_{\text{BN}}(-a + d) - r_{\text{BN}}(a) \geq r_{\text{BN}}(-a + 1) - r_{\text{BN}}(a) = -216a^3 + 324a^2 - 300a + 96$$

and hence  $-216a^3 + 318a^2 - 300a + 96 \leq 0$ , contradicting  $a < 0$ .

- If  $a, b < 0$ , then we can use a similar argument and we obtain that

$$6a^2 = r_{\text{BN}}(a - d) - r_{\text{BN}}(a) > r_{\text{BN}}(a - 1) - r_{\text{BN}}(a) = -144a^3 + 108a^2 - 72a + 12$$

for some positive  $d$  and hence  $-144a^3 + 102a^2 - 72a + 12 < 0$ , implying  $a > 0$ , which is a contradiction.

□

**Lemma 4.5.** *There are no 2-chains of type  $(BN, FR)$ .*

*Proof.* We use a similar strategy as before. Suppose that  $q_{BN}(a) = r_{FR}(b)$  for some  $a, b \in \mathbb{Z}$ . Apart from the trivial solution  $a = b = 0$  we must have  $a = b + d$  for some positive  $d$ . Then

$$q_{BN}(b + d) = q_{BN}(a) = r_{FR}(b) = q_{FR}(b) - 10b^2 - 5b - 2,$$

and hence

$$\begin{aligned} -10b^2 - 5b - 2 &= q_{BN}(b + d) - q_{FR}(b) \\ &\geq q_{BN}(b + 1) - q_{FR}(b) = 11b^4 + 155b^3 + 323b^2 + 296b + 100, \end{aligned}$$

which implies  $11b^4 + 155b^3 + 323b^2 + 301b + 102 \leq 0$ . From this, we can conclude that  $-12 < b < 0$ , we check all these possibilities by hand and see that none of those is possible. □

**Lemma 4.6.** *The only 2-chain of type  $(BN, MNT_3)$  is  $(13, 19, 11)$ .*

*Proof.* We use a similar strategy as before. We know that  $q_{BN}(a) = r_{MNT_3}(b)$  for some  $a, b \in \mathbb{Z}$ . We must have  $a = b + d$  for some non-negative  $d$  (in fact,  $r_{MNT_3}(a) \leq q_{BN}(a)$  exactly on the interval  $[-1, 0]$ ). Then

$$q_{BN}(b + d) = q_{BN}(a) = r_{MNT_3}(b) = q_{MNT_3}(b) - 6b,$$

and hence

$$\begin{aligned} -6b &= q_{BN}(b + d) - q_{MNT_3}(b) \\ &\geq q_{BN}(b + 1) - q_{MNT_3}(b) = 36b^4 + 180b^3 + 336b^2 + 306b + 104, \end{aligned}$$

which implies  $36b^4 + 180b^3 + 336b^2 + 312b + 104 \leq 0$ . From this, we can conclude that  $-3 < b < 0$ , we check all these possibilities by hand and see that the only possibility is  $a = b = -1$ , which corresponds to the chain  $(13, 19, 11)$ . □

#### 4.4 Brute force

For chains of types  $(MNT_4, MNT_3)$  and  $(MNT_6, MNT_3)$ , there are in fact  $a, b \in \mathbb{Z}$  for which  $q(a) = r(b)$  for the respective family polynomials. We will use the fact that the polynomials are quadratic and it is possible to transform them to a generalised Pell equation and then brute force its solutions.

**Lemma 4.7.** *The only 2-chain of type  $(MNT_4, MNT_3)$  with field sizes at most  $2^{5000}$  is the 2-chain specified by  $(5, 7, 11)$ .*

*Proof.* Let  $a, b \in \mathbb{Z}$  be such that

$$a^2 + a + 1 = q_{MNT_4}(a) = r_{MNT_3}(b) = 12b^2 - 6b + 1 \tag{9}$$

By multiplying the equation by 4, we can transform it to a generalised Pell equation  $x^2 - 3y^2 = -2$  for  $x = 2a + 1$  and  $y = 4b - 1$ . Note that  $(2, 1)$  is a solution to  $x^2 - 3y^2 = 1$ , and  $(\pm 1, \pm 1)$  are the only solutions to  $x^2 - 3y^2 = -2$  which satisfy Condition (3) in Theorem 2.4. Furthermore, by Theorem 2.4, we know that  $r, s \in \mathbb{Z}$  is a solution to  $x^2 - 3y^2 = -2$  if and only if there is a  $k \in \mathbb{N}$  such that

$$(2 + \sqrt{3})^k (\pm 1 \pm \sqrt{3}) = r + s\sqrt{3}. \tag{10}$$

For all four possibilities of  $(\pm 1 \pm \sqrt{3})$ , we will show that  $|r|, |s|$  will be increasing with increasing  $k$ .

- For  $1 + \sqrt{3}$ , it is clear that if  $(2 + \sqrt{3})^k(1 + \sqrt{3}) = r + s\sqrt{3}$  and  $(2 + \sqrt{3})^{k+1}(1 + \sqrt{3}) = r' + s'\sqrt{3}$ , then  $|r'| \geq |r|$  and  $|s'| \geq |s|$ .
- For  $-1 - \sqrt{3}$ , it is clear that if  $(2 + \sqrt{3})^k(-1 - \sqrt{3}) = r + s\sqrt{3}$  and  $(2 + \sqrt{3})^{k+1}(-1 - \sqrt{3}) = r' + s'\sqrt{3}$ , then  $|r'| \geq |r|$  and  $|s'| \geq |s|$ .
- For  $1 - \sqrt{3}$ , we see that  $(2 + \sqrt{3})^k(1 - \sqrt{3}) = (2 + \sqrt{3})^{k-1}(-1 - \sqrt{3})$ .
- For  $-1 + \sqrt{3}$ , we see that  $(2 + \sqrt{3})^k(-1 + \sqrt{3}) = (2 + \sqrt{3})^{k-1}(1 + \sqrt{3})$ .

Any  $k, r, s$  satisfying (10) correspond to  $a = \frac{r}{2}$  and  $b = \frac{s+1}{4}$  satisfying (9), hence  $|b|$  is increasing in terms of  $|s|$ . Furthermore, both  $q_{\text{MNT}_3}(x) = 12x^2 - 1$  and  $r_{\text{MNT}_3}(x) = 12x^2 - 6x + 1$  are increasing on  $[1, \infty)$  and decreasing on  $(-\infty, -1]$ .

Thus there are only finitely many  $k$  such that  $\max(q_{\text{MNT}_3}(b), r_{\text{MNT}_3}(b)) < 2^{5000}$ . We enumerated all such  $k$ , and checked that for each one, at least one of the corresponding  $r_{\text{MNT}_4}(a)$ ,  $q_{\text{MNT}_4}(a)$ ,  $q_{\text{MNT}_3}(b)$  is composite, except for the 2-chain specified by (5, 7, 11).  $\square$

**Lemma 4.8.** *The only 2-chains of type  $(\text{MNT}_6, \text{MNT}_3)$  with field sizes at most  $2^{5000}$  are the 2-chains specified by (31, 37, 47) and (43, 37, 47).*

*Proof.* This proof is analogous to the proof of Theorem 4.7. Let  $a, b \in \mathbb{Z}$  such that

$$4a^2 + 1 = q_{\text{MNT}_6}(a) = r_{\text{MNT}_3}(b) = 12b^2 - 6b + 1 \quad (11)$$

We use the same trick as before. Multiply the equation by 4 transform it to  $x^2 - 3y^2 = -3$  for  $x = 4a$  and  $y = 4b - 1$ . We know that  $r, s \in \mathbb{Z}$  is a solution to this equation if and only if there is a  $k$  such that

$$(2 + \sqrt{3})^k \cdot (0 \pm \sqrt{3}) = r + s\sqrt{3}. \quad (12)$$

For both possibilities of  $0 \pm \sqrt{3}$ ,  $|r|, |s|$  will be increasing with increasing  $k$ .

Any  $k, r, s$  satisfying (12) correspond to  $a = \frac{r}{4}$  and  $b = \frac{s+1}{4}$  satisfying (11), hence  $|b|$  is increasing in terms of  $|s|$ . Again, both  $q_{\text{MNT}_3}(x) = 12x^2 - 1$  and  $r_{\text{MNT}_3}(x) = 12x^2 - 6x + 1$  are increasing on  $[1, \infty)$  and decreasing on  $(-\infty, -1]$ .

Thus there are only finitely many  $k$  such that  $\max(q_{\text{MNT}_3}(b), r_{\text{MNT}_3}(b)) < 2^{5000}$ . We enumerated all such  $k$ , and checked that for each one, at least one of the corresponding  $r_{\text{MNT}_6}(a)$ ,  $q_{\text{MNT}_6}(a)$ ,  $q_{\text{MNT}_3}(b)$  is composite, except for the 2-chains specified by (31, 37, 47) and (43, 37, 47).  $\square$

## 4.5 2-adicity

**Lemma 4.9.** *There are no SNARK-friendly 2-chains of prime order curves where the inner curve is in the  $\text{MNT}_3$  family.*

*Proof.* We need that  $2^L \mid q_{\text{MNT}_3}(a) - 1 = 12a^2 - 2 = 2(6a^2 - 1)$ , hence  $L \leq 1$  and hence the outer curve has too small 2-adicity.  $\square$

## 4.6 Summary

We summarize the results of this whole sections as follows. Note that except for the  $(\text{MNT}_3, \text{FR})$  type, we never needed the 2-adicity condition.

**Theorem 4.10.** *The only 2-chains of prime-order elliptic curves from combination of  $\text{MNT}$ ,  $\text{FR}$ , and  $\text{BN}$  families are*

- of type  $(\text{MNT}_4, \text{MNT}_6)$  or  $(\text{MNT}_6, \text{MNT}_4)$ ,
- of type  $(\text{MNT}_3, \text{FR})$ , in which case the 2-adicity of the second curve is at most 1,

**Table 2:** Small 2-chains from combinations of the mentioned families.

Type	$a$	$b$	$r_1$	$q_1 = r_2$	$q_2$
(4, 3)	2	1	5	7	11
(12, 3)	-1	-1	13	19	11
(4, 12)	3	-1	17	13	19
(6, 3)	3	2	43	37	47
(6, 3)	-3	2	31	37	47

- of type  $(MNT_4, MNT_3)$  or  $(MNT_6, MNT_3)$  and field sizes at least  $2^{5000}$ , or
- mentioned in Table 2.

**Corollary 4.11.** *The only SNARK-friendly 2-chains from combination of MNT, FR, and BN families with field sizes at least 50 and at most  $2^{5000}$  are of type (4, 6), or (6, 4).*

## 5 Related work

Ben-Sasson et al. [BSCTV14] first introduced cycles of pairing-friendly elliptic curves in 2014 as a tool to solve problems in modern zero-knowledge protocols, such as zk-SNARKs. However, finding such cycles seems difficult in general.

Karabina and Teske [KT08] showed that 2-cycles of type (4, 6) are easy to find in the MNT family of curves. To this day, this remains the only known way to efficiently construct 2-cycles of pairing-friendly curves. However, in practice, these curves have too small embedding degrees, so large parameters  $q, r$  are needed to obtain a reasonable security level, leading to very long computations. Finding new constructions of cycles of pairing-friendly curves would help implement zk-SNARKs (and potential future protocols) more efficiently.

Chiesa et al. [CCW19] proved that the only 2-cycles consisting only of MNT curves are of type (4, 6), and ruled out any 2-cycles of type (5, 10), (8, 8), and (12, 12). They also showed that there are no 2-cycles consisting only of Freeman curves or only of BN curves and asked if there are any  $m$ -cycles of combinations of MNT, Freeman and BN curves. This question has been answered for  $m = 2$  by us [Nov17] and independently by Bellés-Muñoz et al [BMUS23] (see Theorem 3.4).

## 6 Conclusions

In this work, we prove (Theorem 3.3) that every family  $\mathcal{F}$  of prime-order elliptic curves satisfies at least one of the following:

- there is a  $k$  such that all but finitely many curves in the family are in a  $(\mathcal{F}, k)$ -cycle, or
- all cycles of type  $(\mathcal{F}, k)$  contain curves with field size  $q \in \Omega(\log k)$ .

For  $\mathcal{F}$  being one of the MNT3, Freeman, and BN families, we computed the implied constants explicitly and found that *there are no pairing-friendly 2-cycles of type  $(\mathcal{F}, k)$  for any  $k$ .*

We should note that the definition of pairing-friendliness was established somewhat arbitrarily (as discussed in [FST10]), and some authors, including [BK98], also consider curves with embedding degree  $O((\log q)^2)$  to be pairing-friendly. It remains unclear whether there are 2-cycles of curves where one curve is in a known prime-order family and the other has embedding degree slightly larger than  $\frac{\log_2 q}{8}$ . This could be particularly interesting in the case of the Freeman family, as our result does not rule out the existence of 2-cycles where the second embedding degree  $k$  is slightly larger than  $\frac{\log_2 q}{7.2} - 10$ .

One of the ideas to overcome the problem of constructing pairing-friendly 2-cycles is to use SNARK-friendly chains of elliptic curves [EHG22].

However, our Theorem 4.11 shows that there are no cryptographically relevant SNARK-friendly 2-chains containing curves only from the MNT, Freeman, and Barreto-Naehrig families (except for the (MNT4, MNT6)-chains).

There are ways to overcome the problem that we cannot create useful 2-cycles or 2-chains. For example, [BGH19] and [Hop] avoid pairings and drop the pairing-friendly requirement, and [EHG22] uses non-prime-order curves. We refer the reader to [AHG23] for details.



## References

- [AHG23] Diego F. Aranha, Youssef El Housni, and Aurore Guillevic. A survey of elliptic curves for proof systems. 91(11):3333–3378, 2023. doi:10.1007/s10623-022-01135-y.
- [BGH19] Sean Bowe, Jack Grigg, and Daira Hopwood. Halo: Recursive proof composition without a trusted setup. Cryptology ePrint Archive, Report 2019/1021, 2019. <https://eprint.iacr.org/2019/1021>.
- [BK98] R. Balasubramanian and Neal Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under the Menezes - Okamoto - Vanstone algorithm. 11(2):141–145, March 1998. doi:10.1007/s001459900040.
- [BMUS23] Marta Bellés-Muñoz, Jorge Jiménez Urroz, and Javier Silva. Revisiting cycles of pairing-friendly elliptic curves. pages 3–37, 2023. doi:10.1007/978-3-031-38545-2\_1.
- [BN06] Paulo S. L. M. Barreto and Michael Naehrig. Pairing-friendly elliptic curves of prime order. pages 319–331, 2006. doi:10.1007/11693383\_22.
- [BSCTV14] Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, and Madars Virza. Scalable zero knowledge via cycles of elliptic curves. In *CRYPTO 2014*, pages 276–294. Springer, 2014.
- [CCW19] Alessandro Chiesa, Lynn Chua, and Matthew Weidner. On cycles of pairing-friendly elliptic curves. *SIAM Journal on Applied Algebra and Geometry*, 3(2):175–192, 2019.
- [Con17] Keith Conrad. Pell’s equation, II, [accessed 2025-04-17]. URL: <https://kconrad.math.uconn.edu/blurbs/ugradnumthy/pelleqn2.pdf>.
- [Cox13] D.A. Cox. *Primes of the Form  $x^2 + ny^2$ : Fermat, Class Field Theory, and Complex Multiplication*. Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. Wiley, 2013.
- [DF04] David S. Dummit and Richard M. Foote. *Abstract algebra*. Wiley, 3rd ed edition, 2004.
- [EHG22] Youssef El Housni and Aurore Guillevic. Families of SNARK-friendly 2-chains of elliptic curves. pages 367–396, 2022. doi:10.1007/978-3-031-07085-3\_13.
- [Fre06] David Freeman. Constructing pairing-friendly elliptic curves with embedding degree 10. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Algorithmic Number Theory*, pages 452–465, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.
- [FST10] David Freeman, Michael Scott, and Edlyn Teske. A taxonomy of pairing-friendly elliptic curves. 23(2):224–280, April 2010. doi:10.1007/s00145-009-9048-z.
- [GG13] Joachim von zur Gathen and Jrgen Gerhard. *Modern Computer Algebra*. Cambridge University Press, USA, 3rd edition, 2013.
- [HJ12] Roger A Horn and Charles R Johnson. *Matrix analysis*. Cambridge university press, 2012.
- [Hop] D. Hopwood. The pasta curves for halo 2 and beyond. URL: <https://electriconcoin.co/blog/the-pasta-curves-for-halo-2-and-beyond/>.

- [KTo8] Koray Karabina and Edlyn Teske. On prime-order elliptic curves with embedding degrees  $k = 3, 4$ , and  $6$ . In Alfred J. van der Poorten and Andreas Stein, editors, *Algorithmic Number Theory*, pages 102–117, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg.
- [MNT01] Atsuko Miyaji, Masaki Nakabayashi, and Shunzo Takano. Characterization of elliptic curve traces under FR-reduction. pages 90–108, 2001. doi: [10.1007/3-540-45247-8\\_8](https://doi.org/10.1007/3-540-45247-8_8).
- [Nov17] Tomáš Novotný. Cycles of pairing-friendly elliptic curves and their applications in cryptography [online], 2021 [accessed 2025-04-17]. Supervisor : Vladimír Sedláček. URL: <https://is.muni.cz/th/dsib4/>.
- [Was08] L.C. Washington. *Elliptic Curves: Number Theory and Cryptography, Second Edition*. Discrete Mathematics and Its Applications. CRC Press, 2008.