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

Tomáš Novotný

RWTH Aachen University, Aachen, Germany

Abstract. Cryptographic protocols such as zkSNARKs 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 MNT4 and an MNT6 curve. In this work, we prove that a 2-cycle containing an MNT3 curve cannot be pairing-friendly. For other curve families, we have a similar result for cryptographically attractive field sizes. 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 the (MNT4, MNT6) chains.

Keywords: zkSNARKs · Cycles of elliptic curves · Chains of elliptic curves · Pairing-friendly curves · MNT curves · BN curves · Freeman curves

1 Introduction

Pairings of elliptic curves play an important role in the modern zero-knowledge protocols, such as the zk-SNARK protocol. Ben-Sasson et al. [BCTV14] showed how to use *cycles of pairing-friendly elliptic curves* to provide a *scalable* implementation. However, this requires 2-cycles of 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. [1]

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 $|E_1(\mathbb{F}_{q_1})| = q_2$, $|E_2(\mathbb{F}_{q_2})| = q_1$, where q_1, q_2 are primes. We say such cycle is of type (k_1, k_2) if E_1, E_2 are ordinary and k_1, k_2 are the embedding degrees of E_1 and E_2, respectively; recall that an embedding degree of a curve with prime order r is the smallest $k \in \mathbb{N}$ such that r divides $q^k - 1$. For efficiency, we need $k < \frac{\log_2(r)}{8}$; we call such curves *pairing-friendly* [FST06].

Currently, the only method to find a curve with a prescribed embedding degree is to use families of curves [FST06] defined by triples of polynomials that describe the parameters q, r and t of the curve. These parameters determine an elliptic curve up to an isogeny, however, for practical applications, we need to construct the curve explicitly. The only reliable way is the complex multiplication method, which requires the square-free part of $|t^2 - 4q|$ to be small. The current feasible limit for this part is around 10^{16} [BCTV14].

The usage of MNT curves is the only known way to create 2-cycles of pairing-friendly curves [CCW19]. However, 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 during the complex multiplication. Finding new constructions of cycles of pairing-friendly curves would help implement zk-SNARKs (and potential future protocols) more efficiently.

E-mail: tomas.novotny@rwth-aachen.de (Tomáš Novotný)

[1] A part of this work is based on the bachelor's thesis of the author [Nov21]

Date of this document: 2024-10-17.

Karabina and Teske [KT07] showed that 2-cycles of type $(4, 6)$ are easy to find in the MNT family of curves. Chiesa et al. [CCW19] proved that the only 2-cycles consisting only of MNT curves are of type $(4, 6)$, and ruled out any 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 from combinations of MNT, Freeman and BN curves. This has been answered for $m = 2$ by [Nov21] and independently by [BMUS23], showing that for small embedding degrees $k \leq 22$, there are no reasonably sized cycles of elliptic curves containing a curve in the MNT3, Freeman, or BN family, where the other curve has embedding degree k. The authors in [BMUS23] gave explicit bounds on the field size and checked all curves within those bounds. We restate the result of [Nov21] in a compact form, showing similar bounds, which then help us to study the second embedding degree more precisely and prove stronger results.

Contributions and outline

For a 2-cycle $E_1/\mathbb{F}_{q_1}, E_2/\mathbb{F}_{q_2}$ of type (k_1, k_2), where E_1 comes from the MNT3, Freeman or BN curve families, we bound k_2 from below explicitly in terms of q_1 (see Corollary 3.5). This bound appears to be too large, and therefore, 2-cycles consisting of a curve in these families cannot be used in applications that require both curves in the cycle to have a small embedding degree[2] (see Section 3.1). It seems that the lower bound exceeds the upper bound from the definition of pairing-friendly curves, given by [FST06] (see Figure 1). We show our computational result stating that there are no pairing-friendly cycles containing a curve in the MNT3, Freeman or BN family with field sizes less than 2^{4400}. In Section 3.2, we prove this result for all field sizes in the case of the MNT3 family.

In the last chapter, we consider SNARK-friendly chains of elliptic curves and show that there are no reasonably large SNARK-friendly 2-chains containing curves only from the MNT, Freeman, and Barreto-Naehrig families (except for the (MNT4, MNT6)-chains).

2 Preliminaries

2.1 Elliptic curves

Let E be an elliptic curve over a prime order field $\mathbb{F}_q$ (denoted by $E/\mathbb{F}_q$ or just E), denoting the group of points by $E(\mathbb{F}_q)$. A classical result is the Hasse bound [Cox13, Theorem 14.12]:

$$q + 1 - 2\sqrt{q} \leq |E(\mathbb{F}_q)| \leq q + 1 + 2\sqrt{q}.$$

We sometimes call the bounds the Hasse interval of q. Deuring proved (see, for example, [Cox13, Theorem 14.18][3]) that the Hasse bound is tight and dense: for an integer t with $|t| \leq 2\sqrt{q}$, there exists an elliptic curve E over $\mathbb{F}_q$ with precisely $q + 1 - t$ points. Thus given two primes p, q, where p is in the Hasse interval of q, there exists an elliptic curve over $\mathbb{F}_q$ with precisely p points. We call t the *trace of* $E/\mathbb{F}_q$.

The embedding degree of a curve with prime order r is the smallest positive integer k such that r divides $q^k - 1$. For efficiency, we need $k < \frac{\log_2(r)}{8}$, in which case we call the curve *pairing-friendly* [FST06]. The embedding degree can also be described by cyclotomic polynomials.

Lemma 2.1. *[DF04, p. 553] Let k be a positive integer. Then $x^k - 1 = \prod_{d|k} \Phi_d(x)$.*

Lemma 2.2. *[CCW19, Lemma 1,2] Let $E(\mathbb{F}_q)$ have prime order r. Then E has embedding degree k if and only if k is minimal such that r divides $\Phi_k(q)$, or equivalently, r divides $\Phi_k(t - 1)$.*

[2] For example, if $q_1 \geq 2^{256}$, the embedding degree k_2 must be at least 40 in all three mentioned families.

[3] The theorem is much more general, but for our purposes, we only need the consequence for prime fields that we state.

2.2 Families of prime-order curves

To find parameters of elliptic curves, we can use *families of prime-order curves*, which are defined as triplets $\mathcal{F} = (q(x), r(x), t(x))$ of polynomials with rational coefficients satisfying some formal conditions [FST06, Definition 2.7]. We will not specify all the conditions, as we will only use that

$$q(x) \text{ is irreducible,} \qquad \text{and} \qquad r(x) = q(x) + 1 - t(x). \tag{1}$$

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

$$\begin{aligned}
q_{\text{MNT3}}(x) &= 12x^2 - 1, & r_{\text{MNT3}}(x) &= 12x^2 - 6x + 1, & t_{\text{MNT3}}(x) &= 6x - 1,\\
q_{\text{MNT4}}(x) &= x^2 + x + 1, & r_{\text{MNT4}}(x) &= x^2 + 2x + 2, & t_{\text{MNT4}}(x) &= -x,\\
q'_{\text{MNT4}}(x) &= x^2 + x + 1, & r'_{\text{MNT4}}(x) &= x^2 + 1, & t'_{\text{MNT4}}(x) &= x + 1,\\
q_{\text{MNT6}}(x) &= 4x^2 + 1, & r_{\text{MNT6}}(x) &= 4x^2 + 2x + 1, & t_{\text{MNT6}}(x) &= -2x + 1.
\end{aligned}$$

Freeman [FST06] found another family of prime-order elliptic curves with embedding degree 10, and Barreto and Naehrig used a different approach 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.

2.3 Cycles of elliptic curves

Definition 2.3. (Definitions 3 and 4 in [CCW19]) An 2-*cycle of elliptic curves* is a pair of distinct elliptic curves $E_1/\mathbb{F}_{q_1}, E_2/\mathbb{F}_{q_2}$ such that

$$|E_1(\mathbb{F}_{q_1})| = q_2, |E_1(\mathbb{F}_{q_2})| = q_1.$$

We say that an 2-cycle of elliptic curves is *of type* (k_1, k_2), or that it is a (k_1, k_2)-cycle, if all the curves in the cycle are ordinary and $E_i/\mathbb{F}_i$ has embedding degree k_i for each $i = 1, 2$. A $(\mathcal{F}, k')$-*cycle*, or a *cycle of type* $(\mathcal{F}, k')$, is a cycle of elliptic curves E_1, E_2, such that E_1 is in the family $\mathcal{F}$ and E_2 has embedding degree k'.

Lemma 2.4. *[CCW19, Lemma 4] Let $E_1/\mathbb{F}_{q_1}, E_2/\mathbb{F}_{q_2}$ be a 2-cycle of elliptic curves, with traces t_1, t_2 respectively. Then $t_1 + t_2 = 2$.*

Theorem 2.5. *[KT07, Proposition 1] Let $q, r > 64$ be prime numbers. Then the following are equivalent:*

(a) q and r represent an elliptic curve with embedding degree 4 with $|E(\mathbb{F}_q)| = r$,

(b) q and r represent an elliptic curve with embedding degree 6 with $|E(\mathbb{F}_r)| = q$.

2.4 Chains of elliptic curves

In the recent research it becomes more useful not to use cycles to implement recursive proof composition, but only elliptic curve *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 2.6. (Definition 1. in [EHG22]) An m-chain of elliptic curves is a list of distinct curves

$$E_1/\mathbb{F}_{q_1}, \ldots, E_m/\mathbb{F}_{q_m},$$

where $q_1, \ldots, q_m$ are large primes and

$$q_1 = r_2 \mid |E_2(\mathbb{F}_{q_2})|, \ldots, q_{i-1} = r_i \mid |E_i(\mathbb{F}_{q_i})|, \ldots, q_{m-1} = r_m \mid |E_m(\mathbb{F}_{q_m})|.$$

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 $r_i - 1$ for a large $L \geq 1$. We will follow their definition and call these chains SNARK-friendly.

3 Cycles containing a curve from a prime-order family

Let $\mathcal{F} = (q(x), r(x), t(x))$ be a family representing prime-order elliptic curves with embedding degree k and let k' be positive integer. As stated in [BMUS23], either

(a) k' is minimal such that $q_{\mathcal{F}}(x)$ divides $\Phi_{k'}(1 - t_{\mathcal{F}}(x))$ as polynomials, in which case all but finitely many curves in the family $\mathcal{F}$ are in a $(\mathcal{F}, k')$-cycle, or

(b) there are only finitely many $(\mathcal{F}, k')$-cycles.

This motivates the following definition.

Definition 3.1. A family $q(x), r(x), t(x)$ of elliptic curves with embedding degree k is called *cycle-friendly for embedding degree* k' if k' is minimal such that $q(x) \mid \Phi_{k'}(1 - t(x))$ in $\mathbb{Q}[x]$. Otherwise, we call the family *cycle-unfriendly for* k'.

Note that the MNT4 and MNT6 families are cycle-friendly for embedding degrees 6 and 4, respectively. By Definition 3.1, any family is cycle-friendly for at most one embedding degree (it is the minimal k' such that $q(x)$ divides $\Phi_{k'}(1 - t(x))$, if it exists). Therefore, the MNT4 family is not cycle-friendly for any other embedding degree than 6 (and vice versa). On the other hand, as we will see below, there is no k' for which the MNT3, FR, and BN families are cycle-friendly.

Lemma 3.2. *[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 φ is the Euler totient function.*

Corollary 3.3. *All of the families MNT3, FR, BN are cycle-unfriendly for all embedding degrees k.*

Proof. Suppose that the family $\mathcal{F} \in \{\text{MNT3}, \text{FR}, \text{BN}\}$ is cycle-friendly for some k. By definition, $q(x)$ is irreducible, and hence Lemma 3.2 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 $q_{\mathcal{F}}(x) \nmid \Phi_k(1 - t_{\mathcal{F}}(x))$. □

3.1 Lower bound on the embedding degree

We first want to find an upper bound on the field size of the curves in a cycle of type $(\mathcal{F}, k)$, where $\mathcal{F}$ is a cycle-unfriendly family for k. This has already been done in [BMUS23], however, we need to specify the bounds as follows to get a better lower bound on the embedding degree.

Lemma 3.4. *Let $\mathcal{F}$ be a prime-order family with embedding degree k and let k' be an integer for which the family $\mathcal{F}$ is cycle-unfriendly. Write $\Phi_{k'}(1 - t_{\mathcal{F}}(x)) = f(x)q_{\mathcal{F}}(x) + g(x)$ for some polynomials $f(x), g(x) \in \mathbb{Q}[x]$ with $\deg g(x) < \deg q_{\mathcal{F}}(x)$. Let*

$$Q_{\mathcal{F}} \coloneqq \max\{q_{\mathcal{F}}(m) \mid |m| \leq |M|\},$$

where M is the largest real root (in absolute value) of the polynomial

$$d(x) \coloneqq (q_{\mathcal{F}}(x) - g(x))(q_{\mathcal{F}}(x) + g(x)).$$

Then for any $m \in \mathbb{Z}$ for which the elliptic curve specified by $q_{\mathcal{F}}(m)$ and $r_{\mathcal{F}}(m)$ lies in a cycle of type $(\mathcal{F}, k')$, it holds that $q_{\mathcal{F}}(m) \leq Q_{\mathcal{F}}$.

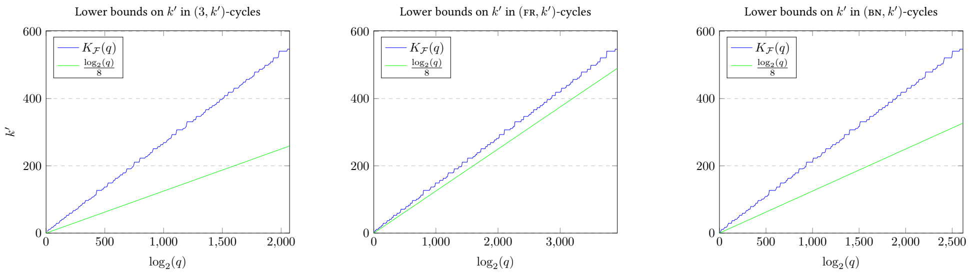

Figure 1: The functions $K_{\mathcal{F}}(q)$ for $\mathcal{F} \in \{\textsc{mnt3}, \textsc{fr}, \textsc{bn}\}$.

Proof. Let $m \in \mathbb{Z}$ be an integer such that the elliptic curve specified by $q_{\mathcal{F}}(m), r_{\mathcal{F}}(m)$ lies in a cycle of type $(\mathcal{F}, k')$. Then $q_{\mathcal{F}}(m) \mid \Phi_{k'}(1 - t(m)) = f(m)q_{\mathcal{F}}(m) + g(m)$ and hence $q_{\mathcal{F}}(m) \mid g(m)$. Since $\mathcal{F}$ is cycle-unfriendly for k', $g(x) \neq 0$, and hence, $|q_{\mathcal{F}}(m)| \leq |g(m)|$. Therefore,

$$0 \geq q_{\mathcal{F}}(m)^2 - g(m)^2 = d(m).$$

Note that the polynomial $d(x)$ is of even degree and has a positive leading coefficient. Therefore,

$$\lim_{x \to \infty} d(x) = \infty, \qquad \text{and} \qquad \lim_{x \to -\infty} d(x) = \infty.$$

It follows that for any $\alpha \in \mathbb{R}$ such that $d(\alpha) \leq 0$ it must hold that $|\alpha| \leq |M|$. Namely, since $d(m) \leq 0$, we have $|m| \leq |M|$. Hence $q_{\mathcal{F}}(m) \leq Q_{\mathcal{F}}$. □

For $k' \in \mathbb{N}$, we define $Q_{\mathcal{F}}(k')$ as the bound $Q_{\mathcal{F}}$ from Lemma 3.4. Given $q \in \mathbb{N}$, we define $K_{\mathcal{F}}(q)$ to be the smallest k such that $Q_{\mathcal{F}}(k) \geq q$. Then by Lemma 3.4, we have the following.

Corollary 3.5. *Let $\mathcal{F}$ be a prime-order family, and $Q \in \mathbb{N}$. Then any $(\mathcal{F}, k')$-cycle of curves with field size at least Q satisfies $k' \geq K_{\mathcal{F}}(Q)$.*

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. [4] We provide an overview of the results in Figure 1. The function $K_{\mathcal{F}}(q)$ is non-decreasing, and hence $K_{\mathcal{F}}(q) \geq 550$ for all $q \geq Q_{\mathcal{F}}(550)$. Therefore, $\frac{\log_2(q)}{8} < 550 \leq K_{\mathcal{F}}(q)$ for all $q < 2^{4400}$. We summarise the computational result in the following proposititon.

Proposition 3.6. *There are no pairing-friendly 2-cycles containing a curve in the MNT3, FR, or BN families, where the curves have field sizes at most 2^{4400}.*

Remark 3.7. It is remarkable how the graphs in Figure 1 seem to be of a linear manner. The dependency in the case of MNT3 family seems to be around $\frac{\log_2 q}{3.79}$, in the case of the Freeman family it is around $\frac{\log_2 q}{7.17}$ and the case of the BN family it is around $\frac{\log_2 q}{4.78}$.

3.2 No pairing-friendly cycles containing an MNT3 curve

In this section, we will use Lemma 3.4 to prove the following result.

Proposition 3.8. *There are no pairing-friendly 2-cycles containing a curve of embedding degree 3.*

We leave the technical proof of the following lemma to the appendix.

[4] To estimate the roots largest real root of the polynomial $d(x)$ we used Theorem 3.10 presented in the next section.

Lemma 3.9. *Let k be a positive integer and use long division of polynomials.*

$$\Phi_k(-6x+2) = (12x^2-1)f(x) + A_k x + B_k.$$

Then $A_k, B_k \in \mathbb{Z}$, $-6 \cdot 2^{2k} < A_k < 0$, and $0 < B_k \leq -\frac{A_k}{2}$.

Furthermore, we will use the following folklore result.

Theorem 3.10 (Upper Bound Theorem). *Let $f(x) \in \mathbb{R}[x]$ be a polynomial with positive leading coefficient, and let $a \geq 0$ be a real number. Write $f(x) = (x-a)q(x) + r$ for some $q(x)$ and $r \in \mathbb{R}$. If $q(x)$ has only positive coefficients and $r \geq 0$, then a is an upper bound on real zeroes of $f(x)$.*

Proof of Proposition 3.8. Let $(3, k)$ be a cycle, where the first curve has field size q. If $q \leq 64$, then $\frac{\log_2(64)}{8} < 1 \leq k$. Otherwise, we can assume that the curve with embedding degree 3 is in the MNT3 family (see [MNT01, Theorem 2]).

Let A_k, B_k be defined as in Lemma 3.9. Clearly,

$$q_{\text{MNT3}}(m) \mid \Phi_k(1 - t_{\text{MNT3}}(m)) \iff q_{\text{MNT3}}(m) \mid A_k m + B_k.$$

Furthermore, let M and $d(x)$ be defined as in Lemma 3.4. Here,

$$d(x) = (12x^2 - A_k x - B_k - 1)(12x^2 + A_k x + B_k - 1).$$

Claim. $M < \sqrt{\frac{2^{8k}+1}{12}} =: X$.

When we have proven the claim, we are done, because

$$k = \frac{\log_2(12X^2-1)}{8} > \frac{\log_2(12M^2-1)}{8} = \frac{\log_2(q_{\text{MNT3}}(M))}{8} = \frac{\log_2(Q_{\text{MNT3}}(k))}{8} \geq \frac{\log_2(q)}{8},$$

since $q_{\text{MNT3}}(x)$ is monotone on $(\infty, 0]$, and $[0, \infty)$. It follows that the cycle is not pairing-friendly.

Equivalently, we need to prove that X is an upper bound on the roots for both the polynomials $12x^2 - A_k x - B_k - 1$ and $12x^2 + A_k x + B_k - 1$. We first show that 2^{4k-2} is an upper bound on roots of both of the polynomials in (a) and (b), respectively.

(a) Long division gives us $12x^2 - A_k x - B_k - 1 = (x - 2^{4k-2})f(x) + g$, where

$$f(x) = 12x + 12 \cdot 2^{4k-2} - A_k, \qquad g = 12 \cdot 2^{8k-4} - 2^{4k-2}A_k - B_k - 1.$$

By Lemma 3.9, $A_k < 12 \cdot 2^{4k-2}$, and $B_k + 1 < 12 \cdot 2^{8k-4} + 2^{4k-1}B_k \leq 12 \cdot 2^{8k-4} - 2^{4k-2}A_k$. By Theorem 3.10, 2^{4k-2} is an upper bound on the real roots of $12x^2 - A_k x - B_k - 1$.

(b) Long division gives us $12x^2 + A_k x + B_k - 1 = (x - 2^{4k-2})f(x) + g$, where

$$f(x) = 12x + 12 \cdot 2^{4k-2} + A_k, \qquad g = 12 \cdot 2^{8k-4} + 2^{4k-2}A_k + B_k - 1.$$

By Lemma 3.9, $A_k > -6 \cdot 2^{2k}$, and

$$12 \cdot 2^{8k-4} + 2^{4k-2}A_k > 12 \cdot 2^{8k-4} + 2^{4k-2}(-6 \cdot 2^{2k}) > 0 \geq -B_k + 1.$$

By Theorem 3.10, 2^{4k-2} is an upper bound on the real roots of $12x^2 + A_k x + B_k - 1$.

Therefore, 2^{4k-2} is a strict upper bound on the real roots of the polynomial $d(x)$. Hence

$$M < 2^{4k-2} < \sqrt{\frac{2^{8k}+1}{12}} = X,$$

which proves the claim. □

4 Chains of curves from prime-order families

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.

Let $(E_1/\mathbb{F}_{q_1}, E_2/\mathbb{F}_{q_2})$ be a 2-chain of prime-order curves over prime fields. Observe that by Definition 2.6 we have that $q_1 \mid |E_2(\mathbb{F}_{q_2})| = r_2$ and since r_2 is prime, $q_1 = r_2$. Therefore, we can view such a 2-chain as a triple of primes (p_1, p_2, p_3), which represents a curve over $\mathbb{F}_{p_2}$ of order p_1 and another curve over $\mathbb{F}_{p_3}$ of order p_2. We will prove the following result.

Proposition 4.1. *The only SNARK-friendly 2-chains from combination of MNT, FR, and BN families are of type* $(4, 6)$, *or* $(6, 4)$.

Since there are 25 possibilities for the type of the 2-chain, we will divide this to various lemmas and propositions depending on the different ways we proved it. We give an overview of the arguments 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 "2ad" means 2-adicity (Section 4.1), "sq" is the squaring argument (Section 4.2), "ineq" is the strategy using inequalities (Section 4.3), and "Pell" uses Pell equation (Section 4.4). Note that MNT4–MNT6 cells are left blank as there are such cycles and hence such chains.

Inner \ Outer	MNT3	MNT4	MNT6	FR	BN
MNT3	2ad	2ad	2ad	2ad	2ad
MNT4	Pell	sq		sq	sq
MNT6	Pell		sq	sq	sq
FR	2ad	2ad	2ad	2ad	2ad
BN	ineq	sq	sq	ineq	ineq

4.1 2-adicity argument

The 2-adicity of the number $r - 1$ in the definition of SNARK-friendly seems to be too strict for the FR and MNT3 family.

Lemma 4.2. *There are no SNARK-friendly 2-chains of prime-order curves where the inner curve is in the FR family.*

Proof. Suppose there is such 2-chain. Then both $q_{\text{FR}}(x) - 1$ and $r_{\text{FR}}(x) - 1$ must be divisible by a large power of 2. It is not difficult to show that for any $L > 0$, $2^L \mid r_{\text{FR}}(x) - 1$ implies $2^L \mid x$, and since $2^L \mid q_{\text{FR}}(x) - 1 = 25x^4 + 25x^3 + 25x^2 + 10x + 2$, we also have $2^L \mid 2$. Therefore, $L \leq 1$ and hence the 2-adicity of the outer curve is too small. □

Lemma 4.3. *There are no SNARK-friendly 2-chains of prime-order curves where the inner curve is in the MNT3 family.*

Proof. Similarly, if there was such 2-chain, $2^L \mid q_{\text{MNT3}}(x) - 1 = 12x^2 - 2 = 2(6x^2 - 1)$, and hence $L \leq 1$, because $6x^2 - 1$ is always odd. □

Note that this means that an equivalent of Proposition 3.8 for the FR family would hold trivially, if we require the pairing-friendly curves to be of high 2-adicity.

Corollary 4.4. *There are no 2-cycles containing a curve from the FR (or MNT3) family, where both curves have 2-adicity at least 2.*

4.2 Squaring argument

In this section, the arguments rely on proving that the equation $q_1(x) = r_2(x)$ asserts that some expression needs to be a perfect square, but we can prove it cannot be.

Lemma 4.5. *Let $\mathcal{F}$ be the MNT4 or MNT6 family. There are no 2-chains of type $(\mathcal{F}, \mathcal{F})$.*

Proof. If $\mathcal{F} = (q(x), r(x), t(x))$ is such family and we have a $(\mathcal{F}, \mathcal{F})$ chain, we know that we must have some $x, y \in \mathbb{Z}$ such that $q(x) = r(y)$.

- MNT4. We must have $x^2 + x + 1 = q_{\text{MNT4}}(x) = r'_{\text{MNT4}}(y) = y^2 + 1$ or $x^2 + x + 1 = q_{\text{MNT4}}(x) = r_{\text{MNT4}}(y) = y^2 + 2y + 2$. In either way, $x^2 + x$ must be a perfect square, which is a contradiction.
- MNT6. Similarly, we must have $4x^2 + 1 = q_{\text{MNT6}}(x) = r_{\text{MNT6}}(y) = 4y^2 + 4y + 1$ and hence $4y^2 + 4y$ must be a perfect square, which is again a contradiction.

□

Lemma 4.6. *There are no 2-chains of type (BN, MNT4).*

Proof. We need that $q_{\text{BN}}(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1$ as to be equal to $r'_{\text{MNT4}}(y) = y^2 + 1$ or $r_{\text{MNT4}}(y) = y^2 + 2y + 2$. In both cases, we need that $q_{\text{BN}}(x) - 1$ is a perfect square. We will show that

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

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

1. $(6x^2+3x+1)^2 = 36x^4+36x^3+21x^2+6x+1 < 36x^4+36x^3+24x^2+6x$ is equivalent to $3x^2 - 1 > 0$, which is true for all integers $x \neq 0$.
2. $36x^4+36x^3+24x^2+6x < (6x^2+3x+2)^2 = 36x^4+36x^3+33x^2+12x+4$ is equivalent to $9x^2 + 6x + 4 > 0$, which is also true for all integers x.

□

Lemma 4.7. *There are no 2-chains of type (BN, MNT6).*

Proof. Since $q_{\text{BN}}(x) = 4y^2 + 2y + 1$, we can multiply both sides by 4 and make the right-hand side a perfect square and we obtain that

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

We need that $K(x)$ is a perfect square. However, it is easy to show that

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

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

Lemma 4.8. *There are no 2-chains of type (MNT4, FR).*

Proof. Assume $q_{\text{MNT4}}(x) = r_{\text{FR}}(y)$. Multiplying both sides by 4 and subtracting 3 makes the left-hand side a perfect square, and we obtain that

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

It is again very easy to show that

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

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

Lemma 4.9. *There are no 2-chains of type* (MNT4, BN).

Proof. Assume $q_{\text{MNT4}}(x) = r_{\text{BN}}(y)$. Multiplying both sides by 4 and subtracting 3 makes the left-hand side a perfect square, and we obtain that

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

It is again very easy to show that

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

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

Lemma 4.10. *There are no 2-chains of type* (MNT6, FR).

Proof. Assume $q_{\text{MNT6}}(x) = r_{\text{FR}}(y)$. Multiplying both sides by 4 and subtracting 4 makes the left-hand side a perfect square, and we obtain that

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

It is again very easy to show that

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

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

Lemma 4.11. *There are no 2-chains of type* (MNT6, BN).

Proof. Assume $q_{\text{MNT6}}(x) = r_{\text{BN}}(y)$. We just need that $r_{\text{BN}}(y) - 1$ is a perfect square. It only suffices to see that

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

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

4.3 Inequality argument

Lemma 4.12. *There are no* 2*-chains of type* (BN, BN).

Proof. Suppose that $q_{\text{BN}}(x) = r_{\text{BN}}(y)$. Clearly, $x, y \neq 0$.

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

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

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

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

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

  again contradicting $x \geq 0$.

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

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

  which contradicts the condition $x \leq 1$.

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

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

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

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

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

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

□

Lemma 4.13. *There are no 2-chains of type (BN, FR).*

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

$$q_{\mathrm{BN}}(y+d) = q_{\mathrm{BN}}(x) = r_{\mathrm{FR}}(y) = q_{\mathrm{FR}}(y) - 10y^2 - 5y - 2,$$

and hence

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

which implies $11y^4 + 155y^3 + 333y^2 + 301y + 102 \leq 0$. From this, we can conclude that $-12 < y < 0$, we check all these possibilities by hand and see that none of those is possible. □

Lemma 4.14. *There are no reasonably large 2-chains of type (BN, MNT3).*

Proof. We use a similar strategy as before. We know that $q_{\mathrm{BN}}(x) = r_{\mathrm{MNT3}}(y)$ for some $x, y \in \mathbb{Z}$. We must have $x = y + d$ for some non-negative d (in fact, $r_{\mathrm{MNT3}}(x) \leq q_{\mathrm{BN}}(x)$ exactly on the interval $[-1, 0]$). Then

$$q_{\mathrm{BN}}(y+d) = q_{\mathrm{BN}}(x) = r_{\mathrm{MNT3}}(y) = q_{\mathrm{MNT3}}(y) - 6y,$$

and hence

$$\begin{aligned} -6y &= q_{\mathrm{BN}}(y+d) - q_{\mathrm{MNT3}}(y) \\ &\geq q_{\mathrm{BN}}(y+1) - q_{\mathrm{MNT3}}(y) = 36y^4 + 180y^3 + 336y^2 + 306y + 104, \end{aligned}$$

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

4.4 Pell equation

The only remaining chain types are $(4, 3)$ and $(6, 3)$. The problem is that in these cases, there are in fact x, y for which $q(x) = r(y)$ for the respective family polynomials. However, we will see that these do not give rise to SNARK-friendly chains. We will use the fact that the polynomials are quadratic and it is possible to transform them to a generalised Pell equation and then study its solutions.

Lemma 4.15. *Let $x, y \in \mathbb{Z}$ are such that $x^2 + x + 1 = q_{MNT4}(x) = r_{MNT3}(y) = 12y^2 - 6y + 1$. Then $7 \mid q_{MNT4}(x)$.*

Proof. By multiplying the equation by 4 one can transform the equation to a generalised Pell equation $a^2 - 3b^2 = -2$ for $a = 2x + 1$ and $b = 4y - 1$. We know that $r, s \in \mathbb{Z}$ is a solution to this equation if and only if there is a k such that

$$(2 + \sqrt{3})^k(1 + \sqrt{3}) = r + s\sqrt{3},$$

which is if and only if there is a k such that

$$\begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}^k \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} r \\ s \end{bmatrix}$$

Claim. For $k \equiv 1, 2 \pmod 4$,

(a) $s \equiv 3 \pmod 4$,

(b) r is odd, and

(c) $r^2 \equiv 4 \pmod 7$.

Proof. It is easy to check that $\begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ when computing modulo 4. Therefore, to prove (a) and (b), it is sufficient to prove it for $k = 1, 2$ (because of the period). But for $k = 1$ is $\begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 3 \end{bmatrix} \pmod 4$ and for $k = 2$ is $\begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}^2 \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 3 \\ 3 \end{bmatrix} \pmod 4$.

For (c), we check that $\begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}^8 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod 7$. Therefore, we must consider cases $k = 1, 2, 5, 6$ and we get that $r \equiv 5, 5, 2, 2 \pmod 7$, respectively, which proves the claim. □

Now, for any solution r, s of the generalised Pell equation, we can use the substitution back to $x = \frac{r-1}{2}$ and $y = \frac{s+1}{4}$ (note that this is possible because of the claim). Therefore, we have infinitely many solutions to $q_{\text{MNT4}}(x) = r_{\text{MNT3}}(y)$. But $x^2 + x + 1 = \frac{r^2+3}{4}$ and since 4 is coprime to 7, we know that $x^2 + x + 1 \equiv r^2 + 3 \equiv 0 \pmod 7$. Therefore, $7 \mid q_{\text{MNT4}}(x)$, which is a contradiction to the fact that $q_{\text{MNT4}}(x)$ is a prime number (unless $q_{\text{MNT4}}(x) = 7$). □

Corollary 4.16. *The only 2-chain of type (MNT4, MNT3) is the chain $(5, 7, 11)$.*

Lemma 4.17. *Let $x, y \in \mathbb{Z}$ are such that $4x^2 + 1 = q_{MNT6}(x) = r_{MNT3}(y) = 12y^2 - 6y + 1$. Then x is odd and $8 \nmid r_{MNT3}(y) - 1$.*

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

$$(2 + \sqrt{3})^k(\sqrt{3}) = r + s\sqrt{3},$$

which holds if and only if there is a k such that

$$\begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}^k \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} r \\ s \end{bmatrix}$$

It is easy to check that $\begin{bmatrix}2 & 3\\1 & 2\end{bmatrix}^k \begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}4\\7\end{bmatrix} \pmod 8$ if and only if $k \equiv 2 \pmod 4$. Therefore, for $k \equiv 2 \pmod 4$, $r \equiv 4 \pmod 8$ and $s \equiv 7 \pmod 8$.

Hence for any solution r, s of the generalised Pell equation, we can use the substitution back to $x = \frac{r}{4}$, but then $x \equiv 1 \pmod 2$.

Furthermore, since x is odd, $r_{\text{MNT3}}(y) - 1 = q_{\text{MNT6}}(x) - 1 = 4x^2$ and hence $8 \nmid r_{\text{MNT3}}(y) - 1$ and the 2-adicity of $r_{\text{MNT3}}(y)$ is at most 2. □

Corollary 4.18. *There are no SNARK-friendly* $($MNT6, MNT3$)$*-chains.*

This concludes the proof of Proposition 4.1.

5 Conclusions

Given a lower bound on the field size and an arbitrary family $\mathcal{F}$ of prime-order elliptic curves, we gave a lower bound on the second embedding degree k in cycles containing a curve from $\mathcal{F}$. In Section 3.2 we proved (in the case of the MNT3 family) that our bound is too strict and is greater than the upper bound on pairing-friendly curves, implying that there are *no pairing-friendly 2-cycles of type* $(3, k)$ *for any* k. It seems reasonable to us to conjecture that the same holds for Freeman and Barreto-Naehrig curves and justify our decision by two criteria: first, we used computational tools to computationally check that this conjecture holds for $q \leq 2^{4400}$; and second, in Appendix B we sketch a possibility how to proceed in the case of arbitrary families. However, we leave this problem unsolved. We mention that today's protocols are not using elliptic curves with field size greater than 2^{4400}, as they would be too slow to work with.

The definition of pairing-friendliness was established somewhat arbitrarily (as discussed in [FST06]), and some authors, including [BK98], also consider curves with embedding degree $O((\log q)^2)$ to be pairing-friendly. Even though our result gives a specific lower bound on the embedding degree, it remains unclear if there are 2-cycles of curves where one curve is in a 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, since in the observed interval (until $q < 2^{4400}$), it would be consistent with our computation that there would be such cycles where the second embedding degree k' is $\frac{\log_2 q}{8} < k' < \frac{\log_2 q}{7}$. We do not provide any results on this matter.

We also prove that there are no (reasonably-sized) SNARK-friendly 2-chains consisting only of curves in the MNT, Freeman, and BN families (except for the $($MNT4, MNT6$)$ chains).

There are multiple ways to overcome the problem that we cannot create cycles or chains as we proposed. For example, [BGH19] and [Hop] avoids pairings and drops 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.

[BCTV14] Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, and Madars Virza. Scalable zero knowledge via cycles of elliptic curves. Cryptology ePrint Archive, Report 2014/595, 2014. https://eprint.iacr.org/2014/595.

[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.

[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.

[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. Cryptology ePrint Archive, Report 2006/026, 2006. https://eprint.iacr.org/2006/026.

[FST06] David Freeman, Michael Scott, and Edlyn Teske. A taxonomy of pairing-friendly elliptic curves. Cryptology ePrint Archive, Report 2006/372, 2006. https://eprint.iacr.org/2006/372.

[Hop] D. Hopwood. The pasta curves for halo 2 and beyond. URL: https://electriccoin.co/blog/the-pasta-curves-for-halo-2-and-beyond/.

[KT07] Koray Karabina and Edlyn Teske. On prime-order elliptic curves with embedding degrees k=3,4 and 6. Cryptology ePrint Archive, Report 2007/425, 2007. https://eprint.iacr.org/2007/425.

[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.

[Nov21] Tomáš Novotný. Cycles of pairing-friendly elliptic curves and their applications in cryptography [online], 2021. Supervisor : Vladimír Sedláček. URL: https://is.muni.cz/th/dsib4/.

A Proof of Lemma 3.9

Lemma A.1. *Let k be a positive integer and use the long division of polynomials.*

$$\Phi_k(x) = (x^2 - 4x + 1)f(x) + a_k x + b_k$$

Then

(a) $0 < a_k$*, and*

(b) $-2a_k < b_k \leq a_k < 4^k$.

Proof. Perform the long division of polynomials.

$$\Phi_k(x) = (x^2 - 4x + 1)f(x) + a_k x + b_k$$

Note that $x^2 - 4x + 1$ is monic, and hence $a_k, b_k \in \mathbb{Z}$.

Since $\Phi_1(x) = x - 1$ and $\Phi_2(x) = x + 1$, we have $a_1 = 1, b_1 = -1$, $a_2 = 1$, and $b_2 = 1$, and both cases satisfy the desired inequalities. Hence we can assume from now that $k > 2$.

By Lemma 2.1, we can write

$$x^k - 1 \equiv \prod_{d|k} (a_d x + b_d) \pmod{x^2 - 4x + 1}.$$

The roots of the polynomial $x^2 - 4x + 1$ are $\alpha := 2 + \sqrt{3}, \beta := 2 - \sqrt{3}$ and therefore,

$$\alpha^k - 1 = \prod_{d|k} (a_d \alpha + b_d), \quad \text{and} \quad \beta^k - 1 = \prod_{d|k} (a_d \beta + b_d)$$

Let us denote

$$\Pi_k^+ := \prod_{\substack{d|k \\ d<k}} (a_d \alpha + b_d), \qquad \Pi_k^- := \prod_{\substack{d|k \\ d<k}} (a_d \beta + b_d)$$

We need to solve (in a_k, b_k) the following system of equations.

$$\alpha^k - 1 = \Pi_k^+ \cdot (a_k \alpha + b_k) \tag{2}$$

$$\beta^k - 1 = \Pi_k^- \cdot (a_k \beta + b_k) \tag{3}$$

Using (3), we express b_k in terms of β, k, Π_k^- and a_k, and plugging into (2) we obtain formula for a_k. Similarly, we also get a formula for b_k.

$$a_k = \frac{\Pi_k^- (\alpha^k - 1) - \Pi_k^+ (\beta^k - 1)}{\Pi_k^+ \Pi_k^- (\alpha - \beta)} \tag{4}$$

$$b_k = \frac{\alpha \Pi_k^+ (\beta^k - 1) - \beta \Pi_k^- (\alpha^k - 1)}{\Pi_k^+ \Pi_k^- (\alpha - \beta)} \tag{5}$$

Let us denote

$$u_k := a_k \alpha + b_k = \Phi_k(\alpha), \qquad v_k := a_k \beta + b_k = \Phi_k(\beta).$$

A simple computation shows that

$$a_k = \frac{u_k - v_k}{2\sqrt{3}}, \qquad b_k = \frac{u_k + v_k}{2} - 2a_k. \tag{6}$$

By the definition of the cyclotomic polynomial,

$$\frac{|v_k|}{|u_k|} = \prod_{\substack{0\le i<k \\ \gcd(i,k)=1}} \frac{|2-\sqrt{3}-\zeta_k^i|}{|2+\sqrt{3}-\zeta_k^i|},$$

where $\zeta_k = e^{\frac{2\pi i}{k}}$ is primitive k-th root of unity in $\mathbb{C}$.

Since $|\zeta_k| = 1$, we have $|2-\sqrt{3}-\zeta_k^i| \le 3-\sqrt{3}$, $|2+\sqrt{3}-\zeta_k^i| \ge 1+\sqrt{3}$. Thus

$$\left|\frac{v_k}{u_k}\right| \le \left(\frac{3-\sqrt{3}}{1+\sqrt{3}}\right)^{\varphi(k)} = (2\sqrt{3}-3)^{\varphi(k)}. \tag{7}$$

Proving (a) is equivalent to showing that $u_k > v_k$. First, note that $\Phi_k(x)$ is positive for any x, since $\Phi_k(0) = 1$ and the polynomial $\Phi_k(x)$ does not have any real roots. In particular,

$$u_k = \Phi_k(2+\sqrt{3}) > 0 \qquad\qquad v_k = \Phi_k(2-\sqrt{3}) > 0.$$

But $\frac{v_k}{u_k} \le (2\sqrt{3}-3)^{\varphi(k)} \le (2\sqrt{3}-3)^2 < 1$, implying $u_k > v_k$ and proving (a).

We will divide (b) into three parts.

- We will prove that $2a_k + b_k > 0$. By (4) and (5), a short calculation shows

$$a_k + b_k = \frac{(2+\sqrt{3})^k - 1}{2\Pi_k^+} - \frac{(2-\sqrt{3})^k - 1}{2\Pi_k^-}.$$

  But from (2) and (3) we see that

$$2a_k + b_k = \frac{a_k(2+\sqrt{3}) + b_k}{2} - \frac{a_k(2-\sqrt{3}) + b_k}{2}.$$

  Showing that this expression is greater than 0 reduces to

$$a_k(2+\sqrt{3}) > a_k(2-\sqrt{3}),$$

  which is trivial from the fact that $a_k > 0$.

- Let us move to the inequality $b_k \le a_k$, or equivalently, $\frac{b_k}{a_k} \le 1$ since a_k is positive. Using (6), we see that

$$\frac{b_k}{a_k} = \frac{-2a_k}{a_k} + \frac{\frac{u_k+v_k}{2}}{\frac{u_k-v_k}{2\sqrt{3}}} = -2 + \sqrt{3}\frac{1+\frac{v_k}{u_k}}{1-\frac{v_k}{u_k}},$$

  so we only need to show that $\frac{1+\frac{v_k}{u_k}}{1-\frac{v_k}{u_k}} \le \sqrt{3}$ in several steps:

$$\frac{1+\frac{v_k}{u_k}}{1-\frac{v_k}{u_k}} = \frac{1+|\frac{v_k}{u_k}|}{1-|\frac{v_k}{u_k}|} \le \frac{1+(2\sqrt{3}-3)^{\varphi(k)}}{1-(2\sqrt{3}-3)^{\varphi(k)}} \le \frac{1+(2\sqrt{3}-3)^2}{1-(2\sqrt{3}-3)^2} \le \sqrt{3}.$$

  The equality holds since $u_k > 0$ and $v_k > 0$. The first inequality holds from (7) and from the fact that the function $\frac{1+x}{1-x} = -1 + \frac{2}{1-x}$ is monotone for any $x \in \mathbb{R}$ on the interval $(-\infty, 1)$. The second inequality comes from the same fact and from $k > 2$, therefore $\varphi(k) \ge 2$. The last inequality is an easy computation.

- The only remaining inequality is $a_k < 4^k$. Note that by (4),

$$a_k = \frac{1-(2-\sqrt{3})^k}{2\Pi_k^-\sqrt{3}} + \frac{(2+\sqrt{3})^k - 1}{2\Pi_k^+\sqrt{3}}.$$

We will prove that $\Pi_k^+ > 1$ and $\Pi_k^- < 0$, implying that the first fraction is negative and therefore

$$a_k < \frac{(2+\sqrt{3})^k - 1}{2\Pi_k^+\sqrt{3}} < (2+\sqrt{3})^k - 1 < 4^k.$$

We proved that $v_k = a_k(2-\sqrt{3}) + b_k > 0$. By definition, Π_k^- is a product of only positive terms and one negative term (namely v_1). Thus, $\Pi_k^- < 0$.

Now let us prove that $\Pi_k^+ > 1$. We proved that $b_k > -2a_k$ and therefore, $a_k(2+\sqrt{3})+b_k > a_k\sqrt{3}$, which is greater than 1, since a_k is a positive integer.

□

Proof of Lemma 3.9. Let $z = -6x + 2$. Then $3(12x^2 - 1) = z^2 - 4z + 1$ and the long division used in the statement of Lemma A.1 becomes

$$\Phi_k(-6x+2) = (12x^2-1) \cdot 3f(x) + a_k(-6x+2) + b_k.$$

Therefore, $A_k = -6a_k$, $B_k = 2a_k + b_k$ and the statement follows. □

B Proposition 3.8 in the case of arbitrary families

At the beginning of the proof of Proposition 3.8, there was nothing special about the polynomials and numbers that showed up. In fact, for any family of prime-order elliptic curves $\mathcal{F} = (q(x), r(x), t(x))$, we can do the following. Let n denote the degree of $q(x)$. Let us perform the long division of polynomials.

$$\Phi_k(1-t(x)) = q(x)f(x) + A_{k,n-1}x^{n-1} + \ldots + A_{k,1}x + A_{k,0}$$

Reducing $(1-t(x))^k - 1 = \prod_{d|k} \Phi_k(1-t(x))$ by $q(x)$, we obtain

$$(1-t(x))^k - 1 \equiv \prod_{d|k}(A_{d,n-1}x^{n-1} + \ldots + A_{d,1}x + A_{d,0}) \pmod{q(x)}.$$

This is equivalent to substituting all the complex roots of $q(x)$; denote them $\alpha_1, \ldots \alpha_n$. Similarly as before, let us denote

$$\Pi_{k,\alpha_i} = \prod_{\substack{d|k \\ d<k}} (A_{d,n-1}\alpha_i^{n-1} + \ldots + A_{d,1}\alpha_i + A_{d,0})$$

Then we have the following equations for each $1 \le i \le n$.

$$(1-t(\alpha_i))^k - 1 = \Pi_{k,\alpha_i} \cdot (A_{k,n-1}\alpha_i^{n-1} + \ldots + A_{k,1}\alpha_i + A_{k,0})$$

This system of n equations is linear for n variables $A_{k,0} \ldots A_{k,n-1}$. Using Cramer's rule and the fact that the matrix of coefficients is Vandermonde, it seems possible to write down formulas for the solutions. For example,

$$A_{k,n} = \frac{\sum_{1\le l\le n}(-1)^{l+1}\frac{(1-t(\alpha_l))^k-1}{\Pi_{k,l}}\prod_{1\le i<j\le n, i\ne l, j\ne l}(\alpha_j - \alpha_i)}{\prod_{1\le i<j\le n}(\alpha_j-\alpha_i)}.$$

Therefore, it should be possible to state some bounds on $A_{k,i}$, which could help us prove that $2^{8k} > Q_{\mathcal{F}}(k)$ (as in Proposition 3.8). For example, we would need to prove something like $A_{k,n} < 36(2^{2k-1.3}+1)$ in the case of the BN family, so that $q_{\text{BN}}(M) < 2^{8k}$.

Nevertheless, such proof would be much longer and much more technical than the proof of Proposition 3.8. It would be much better to find a more straightforward argument; we leave this as an open problem.