Masaryk University
Faculty of Informatics

Cycles of pairing-friendly elliptic curves and their applications in cryptography

Bachelor's Thesis

Tomáš Novotný

Brno, Spring 2021

Masaryk University
Faculty of Informatics

Cycles of pairing-friendly elliptic curves and their applications in cryptography

Bachelor's Thesis

Tomáš Novotný

Brno, Spring 2021

This is where a copy of the official signed thesis assignment and a copy of the Statement of an Author is located in the printed version of the document.

Declaration

Hereby I declare that this paper is my original authorial work, which I have worked out on my own. All sources, references, and literature used or excerpted during elaboration of this work are properly cited and listed in complete reference to the due source.

Tomáš Novotný

Advisor: RNDr. Vladimír Sedláček
Consultant: Mgr. Vojtěch Suchánek

Acknowledgements

This thesis would not be possible without you all. Thank you.

Abstract

Modern zk-SNARK protocols use 2-cycles of elliptic curves, where we often require that the curves are pairing-friendly and have a high 2-adicity. The only known pairing-friendly cycles come from the MNT4 and MNT6 families; however, they are ineffective.

This work shows that a 2-cycle containing an MNT3 curve cannot be pairing-friendly; for other families, we have a similar result for cryptographically attractive field sizes. Therefore, it is necessary to choose another method of creating pairing-friendly 2-cycles in these protocols. We also describe the 2-adicity of all known pairing-friendly families of prime-order curves.

Abstrakt

Moderní zero-knowledge protokoly zk-SNARKs využívají 2-cykly eliptických křivek, kde často požadujeme, aby příslušné křivky byly pairing-friendly a měly vysokou 2-adicitu. Jediné známé pairing-friendly cykly pocházejí z rodin MNT4 a MNT6; ty však nejsou dostatečně efektivní.

V práci ukazujeme, že 2-cyklus obsahující MNT3 křivku nemůže být pairing-friendly; pro další rodiny máme podobný výsledek pro kryptograficky zajímavé velikosti. V protokolech je tedy potřeba zvolit jinou metodu tvorby pairing-friendly 2-cyklů. Také popisujeme 2-adicitu všech známých rodin pairing-friendly křivek prvočíselného řádu.

Keywords

elliptic curve, elliptic curve cycle, family of elliptic curves, cyclotomic polynomial, zk-SNARK

Contents

Introduction

Elliptic curves are currently widely used in cryptography, for example, in the Diffie-Hellman key exchange, digital signatures, or even very promising post-quantum cryptographic protocols based on isogenies. In the recent research of zero-knowledge protocols, elliptic curves prove to be useful as well. Previous implementations of the zk-SNARK protocol are rather expensive and slow. However, Ben-Sasson, Chiesa, Tromer, and Virza [3] showed how to use *cycles of pairing-friendly elliptic curves* to provide a *scalable* implementation (see Chapter 4 for details).

The following definitions are given formally in the next chapters. A pairing-friendly elliptic curve is an elliptic curve that has a *small* embedding degree. In our case, the number of points on the curve r (the *order* of the curve) is a prime number, and thus the embedding degree can be defined as the multiplicative order of its field size q modulo its order r. It is also useful to define the *trace* of the curve as $t = q + 1 - r$. When the order of one curve is the base field size of the other curve and vice versa, we call the curves to be in a 2-cycle. By the *type* of such cycle, we mean a tuple of embedding degrees of the curves in the cycle. The fundamental question is whether it is possible to construct cycles where both curves are pairing-friendly.

To find the parameters of a curve with a prescribed embedding degree, we can use *families of curves* (in fact, this is the only known way). Freeman, Scott and Teske do an excellent overview and taxonomy of these families in [12]. A family is a triple of polynomials that describe the parameters q, r and t of the curve. That is enough to determine an elliptic curve up to an isogeny, but in practice, we need to construct the curve explicitly.

Currently, the Complex Multiplication method is the only way to construct the curve from q and r. This method requires the curve to have a small CM discriminant[1]. The CM method can be used if the discriminant is not much larger than 10^{16} [3].

1. defined formally in Definition 1.7

Karabina and Teske [19] found that 2-cycles of type $(4, 6)$ can be found easily in the MNT family of curves[2]. Chiesa, Chua, and Weidner [7] assert that the only 2-cycles consisting only of MNT curves are of type $(4, 6)$, and they also rule out types $(5, 10)$, $(8, 8)$, and $(12, 12)$ (there are *no* cycles of this type).

The only known way to construct cycles of pairing-friendly curves is the usage of MNT curves. However, these curves have too small embedding degrees, and large parameters are needed to obtain a reasonable security level. Also, these curves have increasing discriminant with increasing base field size, which leads to very long computations to achieve the curve from the parameters q and r. Therefore, it would be useful to find other constructions of cycles of pairing-friendly curves to implement zk-SNARKs (and maybe some other future protocols) more efficiently.

The Sage implementation of the algorithms we use in this work is available on `https://gitlab.fi.muni.cz/xnovot16/cycles`. A copy of the repository is available as an attachment.

Contributions of this work

- **2-adicity.** For applications, we also need the curves to be highly 2-*adic*, which means that $r - 1$ is divisible by a large power of 2. In Chapter 2, we investigate the 2-adicity of known families. We found a new way how to construct highly 2-adic Barreto-Naehrig curves. This could be interesting when choosing a suitable curve for some application under additional assumptions.

- **2-cycles with same embedding degree.** In Chapter 3, we explicitly state which elliptic curves have embedding degree 1 and 2, showing that there are no cycles of type $(1, 1)$ nor $(2, 2)$. We also give an elementary proof in Section 6.3.1 that there are no cycles of type $(4, 4)$. This template can also be used for elementary proof for the case of $(3, 3)$ and $(6, 6)$-cycles.

2. In their paper, they do not explicitly mention cycles, but they found that switching parameters give rise to a bijection between MNT4 and MNT6 for $q, r > 64$.

- **Using families of curves in cycles.** In Chapter 5, we show that in the case of the families of MNT3, Freeman or BN curves, given field size q, there is a lower bound on the second embedding degree in the cycle. 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 [3] (see Chapter 5 for details).

  It seems that the lower bound exceeds the upper bound from the definition of pairing-friendly curves, given by [12] (see Definition 1.16)[4]. Our computation shows that for lower bound on q at most 2^{1200}, and we prove this for all lower bounds in the case of MNT3 curves. This means that *there are no pairing-friendly 2-cycles containing an MNT3 curve*. This statement also seems true for Freeman and BN curves, but we leave this as an open problem.

  We also briefly discuss the case of m-cycles for arbitrary m. Suppose a family of elliptic curves with embedding degree k_1, such that for given integers $k_2, \ldots k_m$, each curve in the family (except finitely many) is in a cycle of type $(k_1, \ldots k_m)$. Then we show that none of the curves has embedding degree 3 (see Section 6.5 for details).

3. For example, for arbitrarily chosen bound $q \geq 2^{256}$, the embedding degree of the other curve must be at least 40 in all three mentioned families.
4. We should mention that they defined this term so as the values fit in some computed values of q and k for given security level (see [12] for details).

1 Elliptic curves over finite fields

For the whole chapter, let $\mathbb{F}_q$ be a finite field of characteristic $p > 3$ and write $q = p^n$. If q is a prime number, we sometimes call this field a *prime field*. We expect the reader to be familiar with the basic properties of finite fields; for more information, one can visit [10, Chapter 13]. We denote the algebraic closure of $\mathbb{F}_q$ as $\overline{\mathbb{F}_q}$.

Definition 1.1. Let $A, B \in \mathbb{F}_q$ satisfy $4A^2 + 27B^3 \neq 0$. An *elliptic curve over* $\mathbb{F}_q$, denoted $E/\mathbb{F}_q$ is a set of points (x, y) with $x, y \in \overline{\mathbb{F}_q}$, the algebraic closure of $\mathbb{F}_q$, satisfying the [5] equation

$$y^2 = x^3 + Ax + B,$$

together with a point $\mathcal{O}$, which is called the *point at infinity*.

Let $\mathbb{F}_{q^k}$ be an extension of $\mathbb{F}_q$. We denote the set of $\mathbb{F}_{q^k}$-rational points on the curve $E/\mathbb{F}_q$ as

$$E(\mathbb{F}_{q^k}) = \{(x, y) \in \mathbb{F}_{q^k} \times \mathbb{F}_{q^k} \mid y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}.$$

Remark. Note that $E/\mathbb{F}_q$ means that E is defined over $\mathbb{F}_q$, and it is the set of points on the curve over $\overline{\mathbb{F}_q}$.

We can define an additive operation on the set of points on an elliptic curve. The idea is to connect two points P, Q with a line that crosses the elliptic curve in a third point $P * Q$, which we connect with the point $\mathcal{O}$ and obtain $P + Q$. By connecting a point to the point at infinity $\mathcal{O}$, we mean drawing a vertical line. [6] When one defines this over the reals and computes the coordinates algebraically (which is done excellently in [24]), one obtains formulas for the addition of points.

It turns out that the elliptic curve together with this operation creates a *commutative group* with identity element $\mathcal{O}$ (a proof is given in [26, Theorem 2.1]). It will be useful for us to denote $[n]P$ (the *scalar multiplication*) the sum on n copies of P, i.e. $[n]P = \underbrace{P + P + \cdots + P}_{n}$.

5. This equation form is called the *short Weierstrass form*

6. It is possible to define the point $\mathcal{O}$ anywhere on the elliptic curve, and one always obtains an associative operation. For more information one can visit [24]. However, this construction is very unnatural, and it is not used; we will not use it either.

In 1934, Hasse proved a very strong bound on the number of points on a curve.

Theorem 1.2. (Theorem 14.12 in [9]) Let E be an elliptic curve over $\mathbb{F}_q$. Then

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

Remark. The proof of this theorem is far beyond the scope of our text, but we can give a brief intuition *why* the number of points should be *near* $q + 1$ (in the case that q is prime). The idea is that given x, the values $x^3 + Ax + B$ are nearly uniformly distributed over $\mathbb{F}_q$ and since there are $\frac{q-1}{2}$ quadratic residues modulo q, we can expect to get about q points, plus the point at infinity $\mathcal{O}$.

In the following text, we often refer to this result as "the Hasse bound" or "the Hasse interval". Deuring proved that the Hasse bound is *tight*. He gave the precise number of the elliptic curves over $\mathbb{F}_p$ having precisely $r = |E(\mathbb{F}_p)|$ points. However, to state his theorem precisely, we would have to dive deep into algebraic number theory, but that is well beyond the scope of our text. The important consequence of his theorem is the following.

Theorem 1.3. (Weak version of Theorem 14.18 in [9]) Let $\mathbb{F}_p$ be a prime field and let t be an integer with $|t| \leq 2\sqrt{p}$. Then there exists an elliptic curve E over the field $\mathbb{F}_p$ with precisely $p + 1 - t$ points.

Remark. Note that Theorem 1.3 does not hold for general finite fields.

Definition 1.4. Let $E/\mathbb{F}_q$ be an elliptic curve. The *trace* of $E(\mathbb{F}_q)$ is defined as an integer t such that $|E(\mathbb{F}_q)| = q + 1 - t$.

Remark. In this setting, the Hasse bound can be restated as $|t| \leq 2\sqrt{q}$.

Definition 1.5. Let $E(\mathbb{F}_q)$ be an elliptic curve with trace t and let p be the characteristic of $\mathbb{F}_q$. We say that E is *ordinary* if p does not divide t. In the other case, we say that E is *supersingular*.

The previous definition, together with Hasse bound, implies the following proposition.

Proposition 1.6. (Proposition 14.15 in [9]) Let $\mathbb{F}_p$ be a prime field and let $E(\mathbb{F}_p)$ be an elliptic curve with number of points r. Then E is supersingular if and only if $r = p + 1$.

It is interesting to note that the case $|E(\mathbb{F}_p)| = p + 1$ is precisely in the middle of the Hasse interval.

Definition 1.7. Let $E(\mathbb{F}_q)$ be an elliptic curve with trace t. The *complex multiplication discriminant of* E is defined as

$$D = \begin{cases} d & \text{if } d \equiv 1 \pmod 4, \\ 4d & \text{otherwise,} \end{cases}$$

where d is the square-free part of the integer $t^2 - 4q$.

Remark. The CM discriminant of E is precisely the fundamental discriminant of the imaginary quadratic field $\mathbb{Q}(\sqrt{d})$, where d is the square-free part of $t^2 - 4q$.

Note that the CM discriminant is always non-positive. This is because the Hasse bound implies that $|t| \leq 2\sqrt{q}$, which means that $t^2 \leq 4q$.

Given the number of points r on a curve and the base prime field $\mathbb{F}_p$, it is possible to construct a curve over $\mathbb{F}_p$ with precisely r points. This is done via the Complex Multiplication method (CM method).

The complex multiplication method [6] is not easy to describe. The crucial step is to compute the Hilbert class polynomial $H_D(x)$, which is beyond the scope of our text to describe. This polynomial can be efficiently computed for *small* values of D (it is feasible if D is less than about 10^{16} [3]). Therefore, for such values of D, we can efficiently construct a curve over $\mathbb{F}_p$ with r points provided that r is in the Hasse interval of p.

Remark. If the CM discriminant of a curve is small, we can do slightly faster scalar multiplication of points on the curve ([15]).

1.1 Torsion points on elliptic curves

Torsion points on an elliptic curve are points with finite order; points P for which there is a positive integer n such that $[n]P = \mathcal{O}$.

Definition 1.8. Let n be a positive integer and let E be an elliptic curve defined over a field $\mathbb{F}_q$. The set of n-torsion points is the set

$$E[n] = \{P \in \overline{\mathbb{F}_q} \times \overline{\mathbb{F}_q} \mid [n]P = \mathcal{O}\} \cup \{\mathcal{O}\}.$$

We denote

$$E[n](\mathbb{F}_{q^k}) = \{P \in \mathbb{F}_{q^k} \times \mathbb{F}_{q^k} \mid [n]P = \mathcal{O}\} \cup \{\mathcal{O}\}.$$

Note that we consider $E[n]$ to contain points over $\overline{\mathbb{F}_q}$. It is easy to see that if $P \in E[n]$ and $Q \in E[n]$, then also $P + Q \in E[n]$ and $-P \in E[n]$, therefore, $E[n]$ is a subgroup of $E(\overline{\mathbb{F}}_q)$.

The notion of an embedding degree will be very important for us.

Definition 1.9. Let $E/\mathbb{F}_q$ be an elliptic curve such that $|E(\mathbb{F}_q)| \neq q$. The *embedding degree of E with respect to a prime divisor $m \neq p$ of $|E(\mathbb{F}_q)|$* is the smallest positive integer k such that m divides $q^k - 1$.

We will often say the *embedding degree of E*, meaning the embedding degree with respect to the largest prime divisor of $|E(\mathbb{F}_q)|$, especially when talking about prime-order curves (curves with $|E(\mathbb{F}_q)|$ being a prime).

Lemma 1.10. [12, Remark 2.2] Let $E/\mathbb{F}_q$ be an elliptic curve and let m be an integer such that m does not divide $q - 1$. Then

$$\left\{ \begin{array}{c} E \text{ has embedding degree } k \\ \text{with respect to } m \end{array} \right\} \iff \left\{ \begin{array}{c} \mathbb{F}_{q^k} \text{ is the smallest extension of } \mathbb{F}_q \\ \text{such that } E[m] \subseteq \mathbb{F}_{q^k} \end{array} \right\}.$$

Remark. If $|E(\mathbb{F}_q)| = q$, the elliptic curve is called *anomalous*. If we want to define embedding degree, we would need to find a positive integer k such that p divides $(p^n)^k - 1$, but that is clearly impossible.

Remark. Supersingular curves have low embedding degrees, namely $k \in \{1, 2, 3, 4, 6\}$ and $k = 2$ for supersingular curves over prime fields $\mathbb{F}_p$ where $p \geq 5$ (see [12, Section 3]).

Let us recall the definition and basic properties of a cyclotomic polynomial.

Definition 1.11. Let k be a positive integer. The *k-th cyclotomic polynomial* is the polynomial

$$\Phi_k(x) = \prod_{\substack{0 \leq i < k \\ \gcd(i,k)=1}} (x - \zeta_k^i),$$

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

Theorem 1.12. ([10, p. 554]) The cyclotomic polynomial $\Phi_k(x)$ is an irreducible monic polynomial in $\mathbb{Z}[x]$ of degree $\varphi(n)$, where φ is the Euler totient function.

As a corollary, we see that $\Phi_k(x)$ is the minimal polynomial for any primitive k-th root of unity over $\mathbb{Q}$.

The roots of $\Phi_k(x)$ are precisely the primitive roots of unity in $\mathbb{C}$. In particular, $\Phi_k(x) \mid x^k - 1$. In fact, the following is true.

Lemma 1.13. Let k be a positive integer. Then

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

Recall that the definition of embedding degree asserts that r divides $q^k - 1$ (where k is the embedding degree, q is the field size, and r is the order of the curve). The following lemma is more specific:

Lemma 1.14. (Lemma 1 in [7]) Let $E(\mathbb{F}_q)$ has prime order r. Then E has embedding degree k if and only if k is minimal such that r divides $\Phi_k(q)$.

This can be further converted into the trace of E.

Lemma 1.15. (Lemma 2 in [7]) Let $E(\mathbb{F}_q)$ has prime order r. Then E has embedding degree k if and only if k is minimal such that r divides $\Phi_k(t-1)$.

As discussed in [12], for applications, it is important that points on the curve have prime order. In the following section, we will see that it is also important that the curves have *a small* embedding degree. We introduce *pairing-friendly curves* as introduced in [12].

Definition 1.16. ([12, Definition 2.3]) We say that an elliptic curve $E(\mathbb{F}_q)$ is *pairing-friendly* if the following two conditions hold:

(a) there is a prime $r \geq \sqrt{q}$ dividing $|E(\mathbb{F}_q)|$, and

(b) the embedding degree of E with respect to r is less than $\frac{\log_2(r)}{8}$.

For example, a prime-order curve with $q \approx 2^{256}$ is pairing friendly if and only if its embedding degree does not exceed 32.

1.2 Pairings

Pairings are a very strong tool and are very often used in cryptography, for example, for three-party one-round key agreement, identity-based encryption, or BLS digital signatures [25]. In zk-SNARKs, it is used as a "homomorphic hiding", which means that it has the homomorphic property for both scalar multiplication and addition of points on an elliptic curve.

Definition 1.17. [3, Appendix B.1] Let G_1, G_2 be cyclic groups (written often in additive notation) of prime order r and let g_1 and g_2 be generators of G_1, G_2 respectively. Let G_T be a cyclic group (written often in multiplicative notation) of order r. A *pairing* is a map $e : G_1 \times G_2 \to G_T$, such that it is

- *bilinear*. For any $\alpha, \beta \in \mathbb{Z}/r\mathbb{Z}$ it holds

$$e(\alpha g_1, \beta g_2) = e(g_1, g_2)^{\alpha\beta}$$

- *non-degenerate*. The element $e(g_1, g_2)$ is not the identity of G_T.

If $G_1 = G_2$, we call the pairing *symmetric*.

Remark. In applications, we often require the pairing e to be efficiently computable.

Such pairings are often regarded as a *black-box* when describing a cryptographic protocol at a high level.

These pairings are often instantiated by Tate or Weil pairing, which use elliptic curves. If pairing-friendly elliptic curves are used, the Tate and Weil pairings are also efficiently computable.

Proposition 1.18. ([26, Theorem 3.9]) Let E be an elliptic curve over $\mathbb{F}_q$ and let n be a positive integer, such that the p (the characteristic of $\mathbb{F}_q$) does not divide n. Denote $\overline{\mu_n} = \{x \in \overline{\mathbb{F}_q} \mid x^n = 1\}$ the group of n-th roots of unity in $\overline{\mathbb{F}_q}$. Then there is a symmetric pairing, called the *Weil pairing*:

$$e_n : E[n] \times E[n] \to \overline{\mu_n}.$$

Furthermore, this pairing satisfies:

(a) $e_n(T,T) = 1$ for all $T \in E[n]$,

(b) $e_n(T,S) = e_n(S,T)^{-1}$ for all $S,T \in E[n]$

If we consider the curve over a finite field $\mathbb{F}_q$ and the embedding degree of E is k, then if m does not divide $q-1$, we know that the full m-torsion is defined over $\mathbb{F}_{q^k}$. It can be proven that then $\overline{\mu_m} \subseteq \mathbb{F}_{q^k}$ ([26, Corollary 3.11]).

The Weil pairing is widely used in the study of elliptic curves and cryptography. For example, it is used to prove the Hasse bound.

The elliptic curves over finite fields have another pairing, called the *Tate-Lichtenbaum pairing*.

Proposition 1.19. [26, Theorem 3.17] Let E be an elliptic curve over $\mathbb{F}_q$ and choose positive integers n,k such that $n \mid q^k - 1$ and $E(\mathbb{F}_{q^k})[n]$ is non-trivial. Denote

$$\mu_n = \{x \in \mathbb{F}_{q^k} \mid x^n = 1\}$$

and let $P \in E(\mathbb{F}_{q^k})[n]$. Let $Q \in E(\mathbb{F}_{q^k})$ and choose $R \in E(\overline{\mathbb{F}_{q^k}})$ satisfying $nR = Q$. Let e_n denote the n-th Weil pairing and $\phi = \phi_{q^k}$ denote the q^k-th power Frobenius endomorphism[7]. Define

$$\tau_n(P,Q) = e_n(P, R - \phi(R)).$$

Then

$$\tau_n : E(\mathbb{F}_{q^k})[n] \times E(\mathbb{F}_{q^k})/nE(\mathbb{F}_{q^k}) \to \mu_n$$

is a well-defined pairing.

The advantage of the Tate-Lichtenbaum pairing over the Weil pairing is the fact that this pairing requires only one point from the n-th torsion to be in $E(\mathbb{F}_q)$ (whereas the Weil pairing requires $E[n] \subseteq E(\mathbb{F}_q)$). Therefore, we can do computations in a smaller extension.

All known pairings (such as Weil, Tate, Ate, Eta, ...) require arithmetic in $\mathbb{F}_{q^k}$ (or some subfield), so k cannot be too large. That is why

7. Given $P = (x,y)$, the Frobenius endomorphism is defined as $\phi_{q^k}(P) = (x^{q^k}, y^{q^k})$. If $P = \mathcal{O}$, then $\phi(P) = \mathcal{O}$.

we need the embedding degree of the curves to be small. On the other hand, k cannot be too small because the pairings provide a reduction of ECDLP [8] to a discrete logarithm problem in $\mathbb{F}_{q^k}^*$ (the MOV attack [26, p. 154]).

8. ECDLP (elliptic curve discrete logarithm problem) is an analogy to the standard discrete logarithm problem. ECDLP states that given an elliptic curve $E/\mathbb{F}_q$ and two points G and $[a]G$ for some integer a, it is *hard* to find the value a.

2 Families of curves

For pairing-based cryptography, we need to generate elliptic curves of a given bit size. This turns out to be possible with polynomials. We can describe the curve field size q and its prime order r by polynomials $q(x)$ and $r(x)$. A *family of prime-order elliptic curves with embedding degree k and CM discriminant D* should be a triple of polynomials $q(x), r(x), t(x)$ such that if these evaluated polynomials in some x define an elliptic curve, then this elliptic curve has embedding degree k and discriminant D.

In practice, the definition of a *family* is slightly more general; as for applications other than cycles, it is not necessary to have prime-order curves. These families are defined similarly, but we do not represent the curve order, but its (possibly the largest) prime divisor. In this work, we stick with this general definition and describe our situation.

Definition 2.1. (Definition 2.5 in [12]) Let $f(x)$ be a polynomial with rational coefficients. We say that f *represents primes* if the following is satisfied:

(a) $f(x)$ is non-constant

(b) $f(x)$ has positive leading coefficient

(c) $f(x)$ is irreducible

(d) $f(x) \in \mathbb{Z}$ for some $x \in \mathbb{Z}$ (equivalently, for an infinite number of $x \in \mathbb{Z}$)

(e) $\gcd\{f(x) \mid x, f(x) \in \mathbb{Z}\} = 1$.

Clearly, these conditions are necessary for f to take an infinite number of prime values, but their sufficiency is an open problem [12].

Definition 2.2. (Definition 2.6 in [12]) A polynomial $f(x) \in \mathbb{Q}[x]$ is integer-valued if $f(x) \in \mathbb{Z}$ for every $x \in \mathbb{Z}$.

Definition 2.3. (Definition 2.7 in [12]) Let $q(x), r(x), t(x) \in \mathbb{Q}[x]$ be non-zero polynomials with rational coefficients. For a given positive integer k and a positive square-free integer D, the triple $\mathcal{F} = (q, r, t)$ *parameterizes a family of prime-order elliptic curves with embedding degree k and discriminant D* if the following is satisfied:

(a) $q(x)$ represents primes.

(b) $r(x)$ is non-constant, irreducible, and integer-valued and has positive leading coefficient.

(c) $r(x)$ divides $q(x) + 1 - t(x)$

(d) k is minimal such that $r(x)$ divides $\Phi_k(t(x) - 1)$

(e) The equation $Dy^2 = t(x)^2 - 4q(x)$ has infinitely many solutions (x, y).

If $\mathcal{F} = (q, r, t)$ is a family and x_0 an integer such that E is an elliptic curve over $\mathbb{F}_{q(x_0)}$ with trace $t(x_0)$, then we say that *E is a curve in the family $\mathcal{F}$*.

Remark. Recall that condition (d) comes from Lemma 1.15 and condition (e) is the CM equation.

These families can be further divided into classes, such as sparse or complete, and others. An excellent overview of known families and classes of elliptic curves can be found in [12].

We are focusing on the families of prime-order curves since we are studying cycles. The only known families of such curves are so-called MNT curves [21], Freeman curves [11] and BN curves [1].

2.1 Families of prime-order curves

To construct families of pairing-friendly elliptic curves, we search for polynomials $q(x), r(x), t(x)$ that satisfy Definition 2.3. Clearly, (q, r, t) describes a family of prime-order curves, if we require $r(x)$ not only to *divide*, but to be *equal* to $q(x) + 1 - t(x)$. Then condition (e) in the definition becomes

(e) $Dy^2 = (t(x) - 2)^2 - 4r(x)$ has infinitely many solutions (x, y).

A crucial observation is that if the right-hand side is a quadratic polynomial $ax^2 + bx + c$, then using the substitution $X = ax + \frac{b}{2}$ it is possible to transform it into a generalized Pell equation $X^2 - aDy^2 = \frac{b^2}{4} - ac$. For any D, for which this equation possesses an integral solution (X, y), we get a family of prime-order pairing-friendly elliptic curves with discriminant D.

Therefore, given polynomials $q(x), r(x)$ and $t(x)$, we can iterate through multiple values of D and find solutions to the generalized Pell equation. The search for curves using this strategy can be further sped up, for example, using a simple observation that $\frac{b^2}{4} - ac$ must be a quadratic residue modulo aD.

Note that if we have linear $t(x)$, we know that $r(x)$ has to be quadratic and therefore it is trivial that $(t(x) - 2)^2 - 4r(x)$ is quadratic. But is there a suitable $t(x)$?

2.1.1 MNT family

Miyaji, Nakabayashi, and Takano [21] described families for embedding degrees $k = 3, 4$ and 6 (See Table 2.1). These families are sometimes denoted MNT3, MNT4 and MNT6.

For example, whenever both $q(x) = 12x^2 - 1$ and $r(x) = 12x^2 - 6x + 1$ are prime numbers for some x, we have an elliptic curve with embedding degree 3 represented by these numbers. [9].

Surprisingly, the converse is also true. This means that *every* elliptic curve (with $q > 64$) of embedding degree $3, 4$ or 6 is of this form. In particular, we have the following result.

Theorem 2.4. (Theorems 2, 3, 4 in [21]) Let q be a prime, and let $E/\mathbb{F}_q$ be an ordinary elliptic curve such that $r = \#E(\mathbb{F}_q)$ is prime. Let $t = q + 1 - r$.

(a) Suppose $q > 64$. Then E has embedding degree $k = 3$ if and only if there exists $x \in \mathbb{Z}$ such that $t = -1 \pm 6x$ and $q = 12x^2 - 1$.

9. In our setting, there are a few exceptions; for example, the curve represented by $q = 5, r = 3$, which fits as a result of the polynomials for MNT6 in the point -1, has embedding degree 2, not 6. Theorem 2.4 formalizes this and we see that this construction is guaranteed to work for $q > 64$.

(b) Suppose $q > 36$. Then E has embedding degree $k = 4$ if and only if there exists $x \in \mathbb{Z}$ such that $t = -x$ or $t = x + 1$, and $q = x^2 + x + 1$.

(c) Suppose $q > 64$. Then E has embedding degree $k = 6$ if and only if there exists $x \in \mathbb{Z}$ such that $t = 1 \pm 2x$ and $q = 4x^2 + 1$.

Table 2.1: MNT family

k	$q(x)$	$r(x)$	$t(x)$
3	$12x^2 - 1$	$12x^2 - 6x + 1$	$6x - 1$
4	$x^2 + x + 1$	$x^2 + 2x + 2, x^2 + 1$	$-x, x + 1$
6	$4x^2 + 1$	$4x^2 + 2x + 1$	$-2x + 1$

Unfortunately, it is not possible to generate arbitrarily large MNT curves with a fixed CM discriminant. In fact, for fixed D, there exist only finitely many MNT curves with discriminant smaller or equal to D ([12], discussion at the end of Section 5.1.)

Remark. The fact that CM discriminants of MNT curves grow is quite essential. In the next chapter, we will see that the only known possibility to create cycles of elliptic curves is the usage of MNT curves. However, since they have large discriminants, it is very expensive to find the curves explicitly (because the CM method requires small discriminants).

So far, we discussed the case where $\varphi(k) = 2$, where φ is the Euler totient function. For $\varphi(k) > 2$ it is extremely unlikely that the right-hand side of the CM equation is quadratic ([12]). However, Freeman discovered an example of such behaviour for embedding degree 10.

2.1.2 Freeman family

Freeman's construction relies on the following factorization of the polynomial $\Phi_{10}(10x^2 + 5x + 2)$, discovered originally in [14]:

$$(400x^4 + 400x^3 + 240x^2 + 60x + 11)(25x^4 + 25x^3 + 15x^2 + 5x + 1).$$

If we set $r(x)$ to be the second factor and $t(x) = 10x^2 + 5x + 3$, we have

$$(t(x) - 2)^2 - 4r(x) = -15x^2 - 10x - 3.$$

Therefore, we can transform the CM equation $Dy^2 = -15x^2 - 10x - 3$ into a generalized Pell's equation

$$X^2 + 15Dy^2 = -20.$$

We see that for any non-positive integer D for which the last equation has an integral solution, we have a family of prime-order curves with embedding degree 10 and discriminant D.

To conclude, we mention the polynomials of the Freeman family. Note that the polynomial $q(x)$ is obtained as $r(x) + t(x) - 1$.

$$\begin{aligned} q(x) &= 25x^4 + 25x^3 + 25x^2 + 10x + 3 \\ r(x) &= 25x^4 + 25x^3 + 15x^2 + 5x + 1 \\ t(x) &= 10x^2 + 5x + 3 \end{aligned}$$

Remark. This construction can be easily transformed for embedding degree 5. Since $\Phi_5(x) = \Phi_{10}(-x)$, we see that $\Phi_5(-10x^2 - 5x - 2)$ factors. Setting $r(x)$ again to $25x^4 + 25x^3 + 15x^2 + 5x + 1$ and $t(x) = -10x^2 - 5x - 1$ leads to the CM equation

$$Dy^2 = 25x^2 + 10x + 5 = 5(5x^2 + 2x + 1).$$

However, the right hand side is always positive, since the polynomial $5x^2 + 2x + 1$ does not have any real roots. Therefore, this equation does not have an integral solution for any non-positive D.

2.1.3 Barreto-Naehrig family

The above construction is not the only possible one. Barreto and Naehrig used a different approach to obtain a family of prime-order elliptic curves. The BN family is represented by the polynomials

$$\begin{aligned} q(x) &= 36x^4 + 36x^3 + 24x^2 + 6x + 1, \\ r(x) &= 36x^4 + 36x^3 + 18x^2 + 6x + 1, \\ t(x) &= 6x^2 + 1. \end{aligned}$$

Short computation shows that the CM equation for the BN polynomials is

$$Dy^2 = 3(6x^2 + 4x + 1)^2,$$

so the right-hand side is not quadratic. However, it is a small factor times a perfect square, exactly what we are looking for. If we set $y(x) = 6x^2 + 4x + 1$ and $D = 3$, we see that the BN polynomials represent a family of prime-order elliptic curves with embedding degree 12 and discriminant 3. Freeman, Scott, and Teske [12] characterize this family as a special case of *sporadic family* and describe it in Section 6.2.

2.2 On the 2-adicity of curves in the families

As shown in [2, p. 24], it is important for efficiency reasons that the used curves are *2-adic*. This means that if the curve has the number of points r, then $r - 1$ is divisible by a large power of two. See Section 4.1.5 for details.

Let us begin with a lemma stating that we only need to consider integers when generating curves using the mentioned families.

Lemma 2.5. Let $\mathcal{F} = (q(x), r(x), t(x))$ be the MNT, Freeman or BN family and let E be an elliptic curve in the family represented by $q = q(l), r = r(l)$. Then $l \in \mathbb{Z}$.

Proof. Let $l = \frac{a}{b}$ be the fraction in lowest terms and suppose that $b \neq 1$.

(a) **MNT3 family.** We know that $t(l) = 6l - 1 \in \mathbb{Z}$. Therefore, $b \in \{2, 3, 6\}$. If $3 \mid b$, then $q(l) = 12l^2 - 1 \notin \mathbb{Z}$ since 9 does not divide 12. Suppose that $b = 2$. Then $q(l) = 12\frac{a^2}{4} - 1 = 3a^2 - 1$, which is even, since a is coprime to $b = 2$. If $a = \pm 1$, then $q(l) = 2$, contradiction.

(b) **MNT4 family.** This is trivial since $t(x) = -x$ or $t(x) = x + 1$.

(c) **MNT6 family.** Since $t(l) = -2l + 1$, $b = 2$. Then $q(l) = 4l^2 + 1 = a^2 + 1$ is even, since a is coprime to $b = 2$.

(d) **Freeman family.** If $t(l) - 3 = 10l^2 + 5l = \frac{10a^2}{b^2} + \frac{5a}{b} \in \mathbb{Z}$, then b^2 must divide $10a + 5b = 5(2a + b)$. In particular, b divides $5(2a + b)$ and therefore, $b = 5$ or b divides $2a$, but b is coprime to a and hence $b = 2$. If $b = 2$, then $t(l) \notin \mathbb{Z}$ and hence $b = 5$. But then $q(l) = 25l^4 + 25l^3 + 25l^2 + 10l + 3 = \frac{1}{25}(a^4 + 5a^3 + 25a^2 + 50a + 75) \in \mathbb{Z}$ and therefore, $5 \mid a$, which is a contradiction, since a and b are coprime.

(e) **BN family.** Since $t(l) = 6l^2 + 1 \in \mathbb{Z}$, then $b^2 \mid 6$, which is impossible for $b > 1$.

□

Definition 2.6. Let n be an integer. The *2-valuation of* n, denoted $\nu_2(n)$, is the highest power of 2 that divides n. More precisely, write $n = 2^k m$ where m is an integer not divisible by 2. Then $\nu_2(n) = k$.

Since we have not found any specification of 2-valuation of curves in mentioned families in the literature, we made a few simple calculations to check the 2-valuation of polynomials $r(x) - 1$ in terms of the 2-valuation of x (see Table 2.2). In the following, we present the computation for MNT and Freeman families.

Proposition 2.7. Let $x \in \mathbb{Z}$. For MNT3, MNT4 and MNT6, we list the 2-valuations of $r(x) - 1$ (note that MNT4 has two possibilities for $r(x)$).

(a) $\nu_2(12x^2 - 6x) = 1 + \nu_2(x)$,

(b) $\nu_2(x^2 + 2x + 1) = 2\nu_2(x + 1)$,

(c) $\nu_2(x^2) = 2\nu_2(x)$,

(d) $\nu_2(4x^2 + 2x) = 1 + \nu_2(x)$.

Proof. (a) Since $12x^2 - 6x = 6x(2x - 1)$ and $2x - 1$ is an odd number, the 2-valuation is $1 + \nu_2(x)$.

(b) We can factor $x^2 + 2x + 1 = (x + 1)^2$ and therefore, the 2-valuation is $2\nu_2(x + 1)$.

(c) This is immediate.

(d) $4x^2 + 2x = 2x(2x + 1)$ and again, $2x + 1$ is odd and therefore, the 2-valuation is $1 + \nu_2(x)$.

□

Table 2.2: 2-adicity of families

Family	$\nu_2(\#E(\mathbb{F}_q)-1)$
MNT3	$1+\nu_2(x)$
MNT4	$2\nu_2(x)$ or $2\nu_2(x+1)$
MNT6	$1+\nu_2(x)$
Freeman	$\max\{1,\nu_2(x)\}$

The following proposition specifies the 2-adicity of Freeman curves.

Proposition 2.8. Let $r(x) = 25x^4 + 25x^3 + 15x^2 + 5x + 1$. Then

$$\nu_2(r(x)-1) = \max\{1, \nu_2(x)\}.$$

Proof. Note that

$$r(x) - 1 = 25x^4 + 25x^3 + 15x^2 + 5x = 5x(5x^3 + 5x^2 + 3x + 1).$$

Suppose that $2 \mid x$. Then $5x^3 + 5x^2 + 3x + 1$ is odd and we see that $\nu_2(r(x)-1) = \nu_2(x)$.

If $x = 2k+1$ for some $k \in \mathbb{Z}$, then

$$5(2k+1)^3 + 5(2k+1)^2 + 3(2k+1) + 1 \equiv 2 \pmod 4.$$

Therefore, $\nu_2(r(x)-1) = 1$. □

The situation with BN curves is a bit different. Let us factor

$$r(x) - 1 = 6x(6x^3 + 6x^2 + 3x + 1).$$

We can see that for even x, the cubic is odd and therefore

$$\nu_2(r(x)-1) = 1 + \nu_2(x).$$

The problem is with the second situation since we cannot make the same argument as in the case of the Freeman family, since when x is odd, the value $6x^3 + 6x^2 + 3x + 1$ might be divisible by 4 (more precisely, it is divisible by 4 if $x \equiv 1 \pmod 4$).

Nevertheless, we can use Hensel's lemma to find odd x's for which the value $r(x) - 1$ has a high 2-valuation. Let us recall Hensel's lemma in its weak form (but it will be enough for us).

Theorem 2.9. (Hensel's lemma) Let p be prime, let $f(x) \in \mathbb{Z}[x]$, and $a \in \mathbb{Z}$ is such that $p \mid f(a)$ and p does not divide $f'(a)$ (f' is the formal derivative of f). Then for any positive integer n, the system of equations

$$\begin{aligned} x &\equiv a \pmod{p} \\ f(x) &\equiv 0 \pmod{p^n} \end{aligned}$$

has a unique solution modulo p^n.

Furthermore, if t_{n-1} is the solution for $f(x) \equiv 0 \pmod{p^{n-1}}$, then there exists unique $0 \leq m < p$ such that

$$f(t_{n-1} + mp^{n-1}) \equiv 0 \pmod{2^n}.$$

□

This is precisely what we are looking for, since we have

$$f(x) = 6x^3 + 6x^2 + 3x + 1,$$

$p = 2$ and $a = 1$.

Proposition 2.10. Let $r(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1$. For any positive integer n there is a unique integer α such that

$$2^n \text{ divides } r(l) - 1 \quad \iff \quad l \equiv \alpha \pmod{2^{n-1}}.$$

for any odd integer l. Furthermore, α can be found very efficiently using Hensel's lemma.

Proof. We see that $r(x) - 1 = 6x(6x^3 + 6x^2 + 3x + 1)$. Let n be an integer. Note that 2 does not divide $f'(x) = 18x^2 + 12x + 3$ for any x. Set α to be the unique solution of the Hensel system of equations

$$\begin{aligned} x &\equiv 1 \pmod{2} \\ 6x^3 + 6x^2 + 3x + 1 &\equiv 0 \pmod{2^{n-1}}. \end{aligned}$$

If $l \equiv \alpha \pmod{2^{n-1}}$, then clearly l is odd and 2^{n-1} divides $6l^3 + 6l^2 + 3l + 1$ and therefore 2^n divides $r(l) - 1$.

For the opposite direction, suppose that 2^n divides

$$r(l) - 1 = 6l(6l^3 + 6l^2 + 3l + 1).$$

Then since l is odd, 2^{n-1} must divide $6l^3 + 6l^2 + 3l + 1$ and from the uniqueness part of Hensel's lemma we get that $l \equiv \alpha \pmod{2^{n-1}}$. □

We computed the value α from Proposition 2.10 for some interesting values of n. The Table 2.3 should be read as follows: 2^n divides $r(l) - 1$ if and only if $l \equiv \alpha \pmod{2^{n-1}}$.

Table 2.3: 2-adicity of Barreto-Naehrig curves

n	α		n	α
34	577309169		45	11090182867441
35	9167243761		48	28682368911857
37	26347112945		49	169419857267185
42	95066589681		51	450894833977841
44	2294089845233		52	1576794740820465

By the second part of Hensel's lemma, this can be computed very efficiently by Algorithm 1 [10].

Algorithm 1: $\mathsf{BN}(n)$

$r(x) \leftarrow 6x^3 + 6x^2 + 3x + 1$
$last \leftarrow 1$
for $i \leftarrow [2..n]$ **do**
  if 2^i *does not divide* $r(last)$ **then**
    $last \leftarrow last + 2^{i-1}$
return *last*

10. This algorithm is implemented in the Git repository attached to this work in file `2-adicity.py` as function `BN(n)`.

3 Cycles of elliptic curves

Let us begin this chapter with an observation about the Hasse interval. Suppose we have an elliptic curve of order r over an unknown field $\mathbb{F}_q$. What are the possible field sizes q, for which r is the order of the curve? After a short calculation we observe that

$$r + 1 - 2\sqrt{r} \leq q \leq r + 1 + 2\sqrt{r}.$$

It turns out that the relation "being in the Hasse interval of" is, in fact, symmetric. This, together with Theorem 1.3 proves the following.

Proposition 3.1. Let r and q be prime numbers. The following are equivalent:

(a) there is an elliptic curve of the order r over the field of size q,

(b) there is an elliptic curve of the order q over the field of size r,

(c) r is in the Hasse interval of q,

(d) q is in the Hasse interval of r.

Proof. Theorem 1.3 implies the equivalences (a)⇔(c) and (b)⇔(d). We will prove (c)⇔(d), and the statement of the proposition will follow. Recall that "r is in the Hasse interval of q" means precisely that $|q + 1 - r| \leq 2\sqrt{q}$. The following are equivalent steps.

$$\begin{aligned} |q + 1 - r| &\leq 2\sqrt{q} \\ q^2 + 2q + 1 - 2qr - 2r + r^2 &\leq 4q \\ q^2 - 2q + 1 - 2qr + 2r + r^2 &\leq 4r \\ |r + 1 - q| &\leq 2\sqrt{r} \end{aligned}$$

The last row is precisely the statement "q is in the Hasse interval of r". □

If the curves from the points (a) and (b) in Proposition 3.1 exist, we call them to be in a *2-cycle*.

Definition 3.2. (Definition 3. in [7]) An *m-cycle of elliptic curves* is a list of m distinct elliptic curves $E_1/\mathbb{F}_{q_1}, \ldots, E_m/\mathbb{F}_{q_m}$ such that

$$\#E_1(\mathbb{F}_{q_1}) = q_2, \#E_1(\mathbb{F}_{q_2}) = q_3, \ldots, \#E_m(\mathbb{F}_{q_m}) = q_1$$

Remark. In [7], the authors also discussed relaxation of this definition, that the number of points on one curve is a multiple of the field size of the next curve. They proved that field sizes of curves in such cycles are bounded from above by $12m^2$, where m is the length of the cycle. This is a very strict bound, and it is not interesting for applications.

For some cryptographic applications, it is required that the curves in the cycle are pairing-friendly, i.e. that the curves have small embedding degrees. [11]

Definition 3.3. (Definition 4. in [7]) We say that an m-cycle of elliptic curves is *of type* $(k_1, k_2, \ldots, k_m)$, or that it is a $(k_1, k_2, \ldots, k_m)$-cycle, if all the curves in the cycle are ordinary and $E_i/\mathbb{F}_i$ has embedding degree k_i for each $i = 1, \ldots, m$.

It is a standard result of Silverman [23, Theorem 5.1], that for any positive integer m, there exists an m-cycle of elliptic curves.

Lemma 3.4. (Lemma 4. in [7]) Let $E_1/\mathbb{F}_{q_1}, \ldots, E_m/\mathbb{F}_{q_m}$ is an m-cycle of elliptic curves, with traces $t_1, \ldots, t_m$ respectively. Then

$$t_1 + \ldots + t_m = m.$$

Proof. Let $n_i = |E(\mathbb{F}_{q_i})|$ for each $i = 1, \ldots, m$. Summing up the equations $n_1 = q_2, \ldots n_m = q_1$ and using $n_i = q_i + 1 - t_i$, we get that $t_1 + \ldots + t_m = m$. □

Proposition 3.5. [7, Proposition 4.] Let $E_1/\mathbb{F}_{q_1}, E_2/\mathbb{F}_{q_2}$ be a 2-cycle of elliptic curves. Then they both have the same discriminant for complex multiplication.

11. However, the current implementation of the protocol Halo does not require the curves to have small embedding degrees.

3.1 Cycles based on MNT curves

In 2008, Karabina and Teske [19] have found an interesting behaviour of the MNT curves with embedding degree 4 and 6.

Theorem 3.6. (Proposition 1 in [19]) Let $q, r > 64$ be prime numbers. Then the following is 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 $\#E(\mathbb{F}_r) = q$.

This property of MNT curves was used in [3] in 2014 to provide a scalable implementation of zk-SNARKs protocols, which we describe in Chapter 4.

In [7], the authors characterized all m-cycles containing only MNT curves.

Proposition 3.7. (Proposition 2 in [7]) If an m-cycle of elliptic curves contains only MNT curves, then it is of type $(4, 6)$ or $(4, 6, 4, 6)$.

In particular, there are no cycles consisting only of MNT curves and containing a curve with embedding degree 3. Furthermore, we have the following corollary.

Corollary 3.8. There are no 2-cycles of type $(3, 3)$, $(4, 4)$ nor $(6, 6)$.

Proof. This follows immediately from the fact that any elliptic curve with embedding degree $3, 4$, or 6 is in the MNT family (see Theorem 2.4). If $q < 64$, we check all the possibilities. □

Remark. An elementary proof (without the use of the fact that any elliptic curve with embedding degree $3, 4$, or 6 is in the MNT family) for $(4, 4)$ cycles (which can be in turn transformed into a proof for $(3, 3)$ and $(6, 6)$ cycles) can be found in Section 6.3.1. Unfortunately, it does not seem to extend to a general case.

3.2 Arbitrary cycles of type (k, k)

Some applications require the curves in a cycle to have a similar embedding degree, but is it possible for them to have the *same* embedding degree? The answer is unknown; if there are some, they have not been discovered yet. Although, there are some results about these cycles. Corollary 3.8 asserts that there are no cycles of type $(3,3)$, $(4,4)$, nor $(6,6)$. In [7], the authors also proved that $(8,8)$ and $(12,12)$ cycles do not exist and their technique sheds some light on the cycles of type $(4k, 4k)$ for all k. [12]

We will extend the list by two more elementary cases, namely $(1,1)$ and $(2,2)$, by explicitly stating which elliptic curves have embedding degree 1 and 2.

Proposition 3.9. Let q, r be prime numbers in the Hasse interval, such that the multiplicative order of q modulo r is 1. Then

$$(q, r) \in \{(3,2), (5,2), (7,3)\}.$$

Proof. From Lemma 1.14 we see that $r \mid q - 1$.

Let $r = q - 1$. Then one of r, q is even and therefore $r = 2, q = 3$. Let $r \neq q - 1$, then $rl = q - 1$ for some $l \geq 2$. Therefore, $r \leq \frac{q-1}{2}$. The Hasse bound asserts $q + 1 - 2\sqrt{q} \leq r$ and thus

$$q + 1 - 2\sqrt{q} \leq \frac{q-1}{2}.$$

This can be simplified to $q \leq 8$. From there, we check all the possibilities and see which r in the Hasse interval of q satisfies $r \mid q - 1$. □

Proposition 3.10. Let q, r be prime numbers in the Hasse interval, such that the multiplicative order of q modulo r is 2. Then

$$(q, r) \in \{(2,3), (5,3), (13,7)\}.$$

12. In fact, on the cycles of type (k, k') where $\Phi_k(x) = \Phi_{k'}(-x)$, which is satisfied also in the case that k is prime and $k' = 2k$.

Proof. Similarly as above, we know that $r \mid q+1$. Let $r = q+1$. Then $q = 2$ and $r = 3$. Now suppose $rl = q+1$ for some $l \geq 2$. Together with Hasse bound this implies

$$q + 1 - 2\sqrt{q} \leq \frac{q+1}{2},$$

which can be simplified to $q \leq 13$. We can again check all the possibilities and find $(5,3)$ and $(13,7)$. □

Corollary 3.11. There is only one prime-order elliptic curve with embedding degree 1, namely

$$E_1/\mathbb{F}_7 : y^3 = x^3 + 4,$$

with precisely three points over $\mathbb{F}_7$.

There are only two prime-order elliptic-curves with embedding degree 2, namely

$$E_2/\mathbb{F}_5 : y^2 = x^3 + 4x + 2,$$
$$E_3/\mathbb{F}_{13} : y^2 = x^3 + 6,$$

with $|E_2(\mathbb{F}_5)| = 3$ and $|E_3(\mathbb{F}_{13})| = 7$.

Comparing the field sizes and the orders, we have the following.

Corollary 3.12. There are no cycles of type $(1,1)$, nor $(2,2)$.

Remark. This corollary can be further generalized. In fact, there are no pairs of prime numbers (p,q) such that the multiplicative order of p modulo q is k and the multiplicative order of q modulo p is k for $k = 1, 2$.

For $k = 1$, we know that $q \mid p-1$ and $p \mid q-1$. Since p, q are positive, we see that $q \leq p-1 \leq q-2$, contradiction.

For $k = 2$, we see that $q \mid p+1$ and $p \mid q+1$, which means that $q \leq p+1 \leq q+2$. Then either $q = p$, which is not possible, since $q \mid p+1$, or $q = p+1$ or $q+2 = p+1$, which gives the only possibility for the primes to be 2 and 3. But the multiplicative order of $p = 3$ modulo $q = 2$ is 1.

4 Protocols using cycles

The elliptic curve pairings from Chapter 1 can be used in cryptographic applications that contain zero-knowledge proofs – proofs of knowledge that do not reveal any unnecessary information. This means that the *prover* can convince the *verifier* that they have some information, but without revealing any new information to the verifier. This becomes very useful when it comes to personal privacy.

These zero-knowledge proofs can be *interactive* or *non-interactive*. Interactive proofs require the prover to be present by the proof, for example, by executing computation that the prover would not be able to compute without knowing the secret. [13]

In a non-interactive zero-knowledge proof, the prover needs to send only a single message to the verifier, and the verifier is convinced about the prover statement. These are often done in the Common Reference String (CRS) model or Random Oracle Model, where some random input for the prover is generated, and the verifier checks the validity of the prover response.

4.1 zk-SNARKs

We can use pairings of pairing-friendly elliptic curves to implement the zero-knowledge Succinct Non-interactive ARgument of Knowledge protocol (zk-SNARK).

On a high level, the zk-SNARK protocol is a tool for the prover to convince the verifier about some valid computation without revealing any secret of the prover (for example, all the computation states; it might contain some prover's personal data).

To understand zk-SNARK protocols more properly, we must define an *arithmetic circuit*.

4.1.1 Arithmetic circuits

One of the first steps is to describe a computation as an arithmetic circuit. We should mention that the zk-SNARK protocol then translates

13. For more information, one can visit the Zero-knowledge Wikipedia page on `https://en.wikipedia.org/wiki/Zero-knowledge_proof`.

this into a quadratic arithmetic program (QAP), which uses polynomials to make the verification very fast. We encourage the reader interested in this topic to read the Zcash blog series at [13], or Chapter 6 in Tran [25].

A $\mathbb{F}_q$-arithmetic circuit is a computational model, which takes inputs in a finite field $\mathbb{F}_q$ and its gates output elements of $\mathbb{F}_q$. They can be represented as directed acyclic graphs with vertices as gates and edges as wires. It is natural to associate an arithmetic circuit with the function it computes.

Definition 4.1. ([25, Definition 6.1]) Let n, h and l be non-negative integers and let D be an acyclic diagram with $+$ and $\times$ gates with $n+h$ inputs and l outputs. Each gate has two input wires and one output wire (corresponding to the fact that $+$ and $\times$ are binary operations). Let $C : \mathbb{F}_q^n \times \mathbb{F}_q^h \to \mathbb{F}_q^l$ be a map such that the image of an $(n+h)$-tuple input is determined by its flow in the diagram D and passage throw the $+$ and $\times$ gates. Then we call the map C a $\mathbb{F}_q$-*arithmetic circuit*.

We divide the input of size $n+h$ to the *input* of size n and the *witness* of size h.

Definition 4.2. ([3, Definition A.1]) Let n, h, l be positive integers respectively denote the input, witness and output size. The *circuit satisfaction problem* of an $\mathbb{F}_q$-arithmetic circuit $C : \mathbb{F}_q^n \times \mathbb{F}_q^h \to \mathbb{F}_q^l$ is defined by the relation

$$\mathcal{R}_C = \{(x, w) \in \mathbb{F}_q^n \times \mathbb{F}_q^h : C(x, w) = 0^l\}.$$

Its language is $\mathcal{L}_C = \{x \in \mathbb{F}_q^n : \exists w \in \mathbb{F}_q^h, C(x, w) = 0^l\}$.

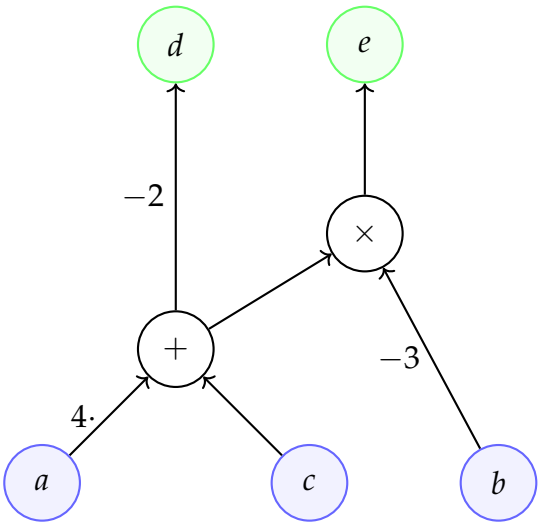
If $(x, w) \in R_C$, we say that (x, w) is a *valid assignment for* C.

Note that if we want the output to be different from 0^l, we can always scale and move the circuit so that our problem will fit the definition.

Example 4.3. Let $C : \mathbb{F}_{13}^2 \times \mathbb{F}_{13} \to \mathbb{F}_{13}^2$ be a $\mathbb{F}_{13}$-arithmetic circuit defined as follows:

$$C((a, b), c) = ((4a + c - 2), (4a + c)(b - 3)).$$

An example of valid assignment for C is $(2, 3, 7)$. The following picture is a graph representation of this circuit. Input nodes are colored blue and output are colored green.



4.1.2 Preprocessing zk-SNARK

Now we are ready to define a zk-SNARK.

Definition 4.4. [3, Section 2.1] A (*preprocessing*) *zk-SNARK* for $\mathbb{F}_q$-arithmetic circuit satisfiability is a triple of polynomial-time algorithms (G, P, V), called the *key generator, prover*, and *verifier*, respectively.

- The key generator G, given a security parameter λ and a $\mathbb{F}_q$-arithmetic circuit $C : \mathbb{F}_q^n \times \mathbb{F}_q^h \to \mathbb{F}_q^l$, samples a *proving key* PK and a *verification key* VK. These are the system's public parameters, which are generated once per circuit.
- Given $(x, w) \in \mathcal{R}_C$, the (honest) prover $P(\text{PK}, x, w)$ produces a proof π for the statement

  "I know a witness w such that $(x, w) \in \mathcal{R}_C$."
- The verifier $V(\text{VK}, x, \pi)$ checks that π is a valid proof for $x \in \mathcal{L}_C$.

There are various implementations of the zk-SNARK protocol (for a list visit [3]). One of the most common are *pairing-based zk-SNARKs* where we use *pairings of pairing-friendly elliptic curves* (as defined in Definition 1.17). The zk-SNARK implementations are very complex to describe, and we do not cover this in the text. We briefly describe how the authors of [3] used cycles of elliptic curves to provide a scalable implementation.

4.1.3 Proof-carrying data systems

Now we move to the work in [3]. Let us fix a predicate Π. Consider a distributed computation, where each node takes input messages and outputs the new message. We need to ensure that all output messages are *compliant* with the predicate Π. Proof-carrying data can fulfil this goal by attaching short and easy-to-verify proofs of Π-compliance to each message.

Definition 4.5. [3, Appendix D] A (*preprocessing*) *proof-carrying data system* (PCD system) for $\mathbb{F}_q$-arithmetic compliance is a triple of polynomial-time algorithms $(\mathbb{G}, \mathbb{P}, \mathbb{V})$, named key-generator, prover and verifier.

- The key-generator $\mathbb{G}$ takes as input a security parameter λ and a $\mathbb{F}_q$-arithmetic compliance predicate Π and creates the proving key $\textsc{pk}$ and verifying key $\textsc{vk}$. We assume that $\textsc{pk}$ contains the predicate Π.
- The prover $\mathbb{P}$ takes as input the proving key $\textsc{pk}$, outgoing message z, local data z_{loc} and incoming messages z_{in} with proof π_{in}, and outputs a proof π for the statement "z is Π compliant".
- The verifier $\mathbb{V}$ takes as input the verification key $\textsc{vk}$, a message z and proof π and outputs 1 if they are convinced by π that z is Π-compliant.

In [3, Section 4], the authors showed how to create a PCD system given two zk-SNARKs, and also how to transform the PCD system to a new scalable zk-SNARK [3, Section 6], as depicted in Figure 4.1.

In the following, we focus on the first part – to construct a PCD system from two zk-SNARKs, since this is where they used cycles of elliptic curves. The main technique used in this construction is called *recursive proof composition*.

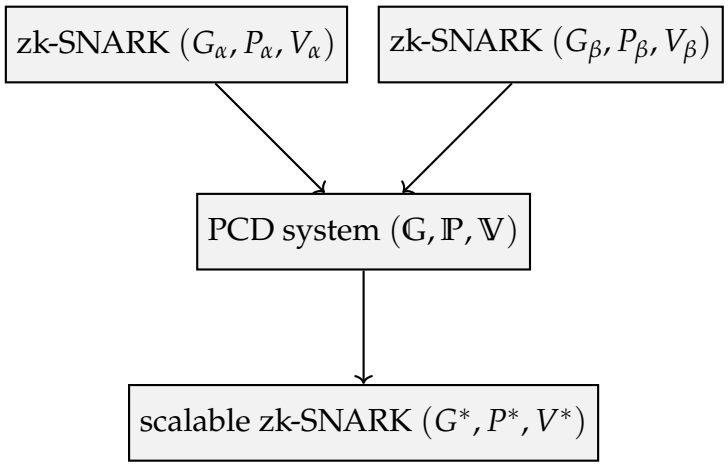
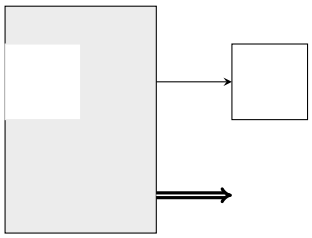


Figure 4.1: Strategy for scalable zk-SNARK

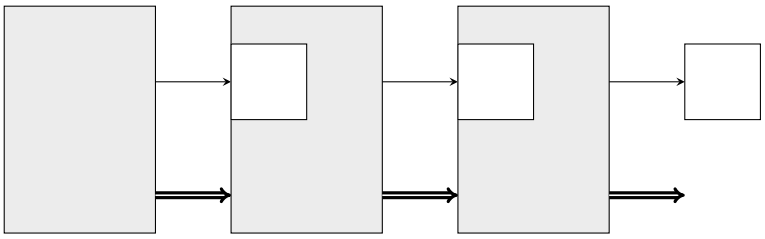
4.1.4 Recursive proof composition

The idea of recursive proof composition is the following. In the first computation step, we provide the output a_1 and create a proof π_1 of Π-compliance. In the second step, we check the proof π_1, provide the output a_2 and create a proof π_2. However, now, it is not needed to hold the proof π_1, since it is "included" in the proof π_2. Therefore, we work only with the latest output and proof.

As a very approximate visual example, a computation step could be depicted as follows.



The grey part contains all the computation (arithmetic circuit). The white space is where the previous proof is verified. Anyone can verify the "white box" heading out, which is the proof for the statement "All the previous proofs are correct and my computation is also correct". The result of the computation is depicted as the double arrow.



Remark. In fact, more computations are merged and verified. Therefore, it is not a linear computation, but in general, it has a structure of a tree.

The preprocessing zk-SNARK performs the proof and verification in one computation step.

As mentioned, in each computation step, we want to include the verification circuit C_V into the PCD circuit C_{pcd}. The problem is the following observation.

If we instantiate a zk-SNARK (G, P, V) with an elliptic curve $E/\mathbb{F}_q$ with prime order r (or order divisible by a large prime r), then

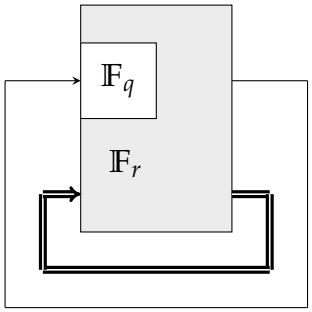
(G, P, V) works for $\mathbb{F}_r$-arithmetic satisfiability, but all of the verifier's computations are over $\mathbb{F}_q$ (or extensions of $\mathbb{F}_q$ up to degree k, where k is the embedding degree of E).[14]

The problem is that we run into a *field mismatch problem*. To prove statements about $\mathbb{F}_r$-arithmetic circuit satisfiability, we instantiate (G, P, V) with a curve $E/\mathbb{F}_q$ such that $|E(\mathbb{F}_q)| = r$ (or more generally, r divides $|E(\mathbb{F}_q)|$). However, then all the verifier's computations are over the field $\mathbb{F}_q$, so we try to embed the $\mathbb{F}_q$-arithmetic circuit into a $\mathbb{F}_r$-arithmetic circuit.

A promising solution would be to use only curves with $q = r$, so-called "anomalous elliptic curves", that could verify its own proofs recursively. However, as discussed in [3], this is not possible for two reasons. First of all, these curves do not have and embedding degree (intuitively, the embedding degree is infinity, leading to inefficient pairings; see Section 1.2 for details). The second problem is that these curves are insecure in the sense that ECDLP on these curves is very

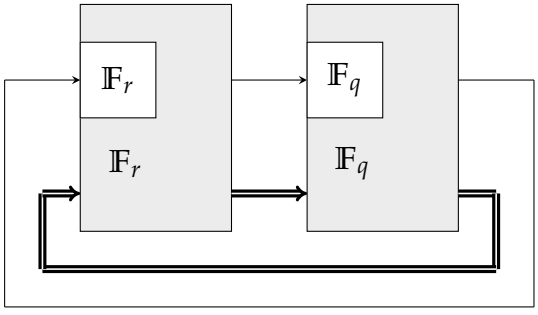
14. This is because we use pairings of elliptic curves. Intuitively, the prover computes some scalar multiples of the points on the curve, which has order r, and therefore, we consider the scalars modulo r. On the other hand, the verifier possesses the values after the pairing, leading to computations over $\mathbb{F}_q$. See [3] for details.

easy. It can be shown that the group structure of anomalous curves over $\mathbb{F}_q$ is isomorphic to $(\mathbb{Z}/_q\mathbb{Z}, +)$, where the discrete logarithm is broken very efficiently using extended Euclidean algorithm. For further details, we refer to [16]. So setting $q = r$ is impossible.



The second idea could be to simulate the $\mathbb{F}_q$-arithmetic using $\mathbb{F}_r$-arithmetic. This approach can be instantiated, but it seems to be expensive [3]. Intuitively, we have to translate the arithmetic circuits into Boolean circuits to simulate the $\mathbb{F}_q$ arithmetic. Therefore, the circuit has to be about $\log q$ times larger.

The fundamental idea of Ben-Sasson, Chiesa, Tromer, and Virza [3] is to use a pair of prime-order elliptic curves for which the base field of the one is equal to the scalar field of the other and vice versa (that is, to use *cycles of elliptic curves*). In this way, the field sizes for particular arithmetic circuits match. A second possibility would be to cycle through multiple curves (see Definition 3.2).



As we saw in the Chapter 3, there is only one known way to construct these cycles (based on MNT curves). However, we are not completely done. These have very small embedding degrees, so the field

sizes have to be really large (about 800 bits) to gain a reasonable security level. However, large field size means slow computation on them (large arithmetic circuits). The second problem regarding these MNT curves is that they have very large CM discriminants, which means that the CM method for determining the curve from its parameters is very costly. In fact, the authors of [3] ran a computation for a couple of months (and spent about 200 core years) to find a suitable cycle for their zk-SNARK implementation.

4.1.5 Suitable parameters of curves for cycles

(a) *Field sizes.* In a 2-cycle of type (k_1, k_2), we want the values k_1, k_2 to be as close as possible, because for different values of k_1, k_2, the ECDLPs in $E(\mathbb{F}_{q_1})$ and in $E(\mathbb{F}_{q_2})$ are unbalanced (because of the different embedding degrees). The bounds on the parameters q_1, q_2 must be considered using the smaller embedding degree. We recall that existence of 2-cycles with same embedding degree is an open problem [7].

(b) *Towering friendliness.* Towering friendly fields are finite fields, for which we can very efficiently construct subfields [4]. It can be shown that the following condition will ensure this need.

Definition 4.6. [4, Definition 2.] Let q be a prime number. We say that a finite field $\mathbb{F}_{q^m}$ is *towering-friendly*, if all prime divisors of m also divide $q - 1$.

Suppose that we have a (k_1, k_2)-cycle of curves and let q_1, q_2 be the field sizes. If the fields $\mathbb{F}_{q_1^{k_1}}$ and $\mathbb{F}_{q_2^{k_2}}$ are both towering friendly, we will obtain faster arithmetic in them [3], which is what we want (those are the field where the pairings are computed). This can be achieved by setting

$$q_1 \equiv 1 \pmod{\operatorname{rad}(k_1)},$$

$$q_2 \equiv 1 \pmod{\operatorname{rad}(k_2)},$$

where $\operatorname{rad}(x)$ is defined as the product of distinct prime divisors of x.

(c) *2-adicity.* As shown in [2, p. 24], it is important for efficiency reasons for the used curve to be 2-adic, that is, that the parameter $r - 1$ is divisible by a large power of two. More precisely, when the key generator is invoked on a circuit C, it is important that $\nu_2(r-1) \geq \log(|C|)$ to hold.

4.2 Project Halo

An up-and-coming project Halo [5] does not require the elliptic curves in the cycles to be pairing-friendly. Halo is the first practical realization of recursive proof composition without a trusted setup. It builds upon a previous project from early 2019 called Sonic, which is a variant of zk-SNARK.

In simple words, Sonic is implemented differently than the preprocessing zk-SNARK presented in the previous section. It uses different techniques, such as polynomial commitment schemes and accumulation schemes. It does not use pairings of elliptic curves, and therefore, it is not needed that the embedding degree is small.

There were several attempts to find suitable curves for a SNARK recursion without pairing-friendly cycles. The first idea was to use half-pairing-friendly cycles, which means that only one curve in the cycle is pairing-friendly[15]. In the end, the search for suitable curves was inspired by a fact about good reduction of elliptic curves with j-invariant 0 discovered in [23].

In the original Halo paper [5], the authors used the following elliptic curves.

$$\text{Tweedledum: } E_{q_1}/\mathbb{F}_{q_1} : y^2 = x^3 + 5$$
$$\text{Tweedledee: } E_{q_2}/\mathbb{F}_{q_2} : y^2 = x^3 + 5$$

where q_1 and q_2 are 255-bit primes:

$$q_1 = 2^{254} + 2^{33} \cdot 5480239103988333266369378 41 + 1$$

$$q_2 = 2^{254} + 2^{34} \cdot 27401195514784876039996517 3 + 1$$

15. An interesting discussion about this topic can be found on `https://github.com/zcash/zcash/issues/4092`.

As we can see, both curves are highly 2-adic, namely 2^{33} divides $q_1 - 1$ and 2^{34} divides $q_2 - 1$.

In 2020, the Electric Coin Company introduced Halo 2 [8]. In the newest implementation, they use PLONK protocol instead of Sonic. They also use different curves (so-called *Pasta curves*).

$$\text{Pallas: } E_{q_1}/\mathbb{F}_{q_1} : y^2 = x^3 + 5$$
$$\text{Vesta: } E_{q_2}/\mathbb{F}_{q_2} : y^2 = x^3 + 5$$

where p and q are 255-bit primes:

$$q_1 = 2^{254} + 2^{32} \cdot 10607837590253843481252147437 + 1$$

$$q_2 = 2^{254} + 2^{32} \cdot 10607837590274021452140702497 + 1$$

There are several computational advantages of the Pallas and Vesta curves over the Tweedle curves [18]. For example, they have the same 2-adicity.

5 Cycles containing a curve from a family

In this chapter, we present our research about cycles containing a curve in a family (in the sense of Definition 2.3).

We begin with two observations [7, Propositions 8. and 9.].

Proposition 5.1. There are no m-cycles consisting only of Freeman curves.

Proposition 5.2. There are no m-cycles consisting only of BN curves.

In [7], the authors also asked if there are any m-cycles from combinations of MNT, Freeman and BN curves. In Section 5.1, we answer this question for $m = 2$ by investigating a bit more general problem: Are there pairing-friendly 2-cycles containing a curve from a family in the sense of Definition 2.3? We will not prove that there are no such 2-cycles (which is not even true; at least there are $(4, 6)$-cycles), although we substantially restrict them. It turns out that neither MNT3 nor Freeman nor BN curves can be a part of 2-cycles with "similar" embedding degrees. More precisely, we show that they are not in a 2-cycle with *any other curve with a low embedding degree* ($k \leq 22$) *for* $q, r > 20$.

We then justify our conjecture (see Conjecture 5.17), stating that if there is some cycle containing a curve in the family of MNT3, Freeman or BN, then the embedding degree of the second curve is "too high", more precisely, that it does not fit in the definition of pairing-friendly curves (see Definition 1.16). In Section 5.3, we conclude this chapter with proof of the conjecture in the case of the MNT3 family.

Let us begin with a lemma.

Lemma 5.3. Let $f(x), g(x) \in \mathbb{Q}[x]$ be polynomials such that $f(x)$ does not divide $g(x)$ in $\mathbb{Q}[x]$. Then there are only finitely many $l \in \mathbb{Z}$ such that $f(l)$ divides $g(l)$ in $\mathbb{Z}$.

Proof. Write $g(x) = h(x)f(x) + r(x)$ where $\deg r(x) < \deg f(x)$ using long division of polynomials. We see that for any $k \in \mathbb{Z}$,

$$f(k) \mid g(k) \iff f(k) \mid r(k).$$

Since $\deg r(x) < \deg f(x)$, for sufficiently large M it holds that $|r(i)| < |f(i)|$ for any i for which $|i| > |M|$. Since $f(x)$ does not divide $g(x)$,

$r(x)$ is not identically zero and it follows that all $l \in \mathbb{Z}$ such that $f(l) \mid g(l)$ satisfy $|l| < |M|$. □

Definition 5.4. Let $\mathcal{F}$ be a family of elliptic curves with embedding degree k and let k' be a positive integer. Suppose there is an elliptic curve E in the family $\mathcal{F}$, which is in a (k, k')-cycle. Then we say that the cycle is a $(\mathcal{F}, k')$-cycle, or a cycle of type $(\mathcal{F}, k')$.

We denote the MNT3 family as MNT3, the Freeman family as FR and the BN family as BN.

Theorem 5.5. 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. Either

(a) all curves in the family $\mathcal{F}$ (except finitely many) are in a $(\mathcal{F}, k')$-cycle, or

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

Proof. 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.

Recall that for any m such that $q(m)$ and $r(m)$ are prime numbers, we know that by Theorem 1.3 we have an elliptic curve specified by $q_1 = q(m), r_1 = r(m), t_1 = t(m)$. By Proposition 3.1, we know that there exists an elliptic curve E' specified as $q_2 = r(m), r_2 = q(m)$, $t_2 = 2 - t(m)$ (the trace can be computed easily from Lemma 3.4). The question is, what is the embedding degree of this curve. Applying Lemma 1.15 on E' we see that E' has embedding degree k' if and only if k' is minimal such that $q_1 = r_2 \mid \Phi_{k'}(t_2 - 1) = \Phi_{k'}(1 - t_1)$. Let us investigate the divisibility $q_1 \mid \Phi_{k'}(1 - t_1)$.

(a) Suppose that the given k' is minimal such that $q(x)$ divides $\Phi_{k'}(1 - t(x))$ as polynomials. Then for any m it holds that

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

but we are not guaranteed that k' is the minimal number with this property. But for any $\bar{k} < k'$, the polynomial $q(x)$ does not divide $\Phi_{\bar{k}}(1 - t(x))$. Therefore, by Lemma 5.3 there are only finitely many m's such that $q(m) \mid \Phi_{\bar{k}}(1 - t(m))$ in $\mathbb{Z}$. Hence

there are only finitely many m's for which k' is not minimal such that $q(m) \mid \Phi_{k'}(1 - t(m))$. For all the other m's, the number k' is minimal for this divisibility, and therefore, by the previous paragraph, the second curve in the cycle has embedding degree k'. Therefore, any curve in the family $\mathcal{F}$ (except finitely many) is in a cycle of type $(\mathcal{F}, k')$.

(b) If k' is not minimal such that $q(x) \mid \Phi_{k'}(1 - t(x))$, but the divisibility holds, clearly there are no cycles of type $(\mathcal{F}, k')$.

(c) The last case is that $q(x)$ does not divide $\Phi_{k'}(1 - t(x))$ as polynomials. By Lemma 5.3, we have only finitely many m's such that
$$q(m) \mid \Phi_{k'}(1 - t(m)),$$
and hence there are only finitely many $(\mathcal{F}, k')$-cycles.

□

5.1 Cycle-friendliness

Theorem 5.5 says that when we fix k' and a family $\mathcal{F}$ of curves defined by polynomials (in the sense of Definition 2.3), then

- all but finitely many curves generated by the family $\mathcal{F}$ give rise to a (k, k')-cycle, or
- there are only finitely many $(\mathcal{F}, k')$-cycles.

Now, we formalize these two cases in the following definition.

Definition 5.6. A family $q(x), r(x), t(x)$ of elliptic curves with embedding degree k is called *2-cycle-friendly for embedding degree k'* if k' is minimal such that
$$q(x) \mid \Phi_{k'}(1 - t(x)).$$
Otherwise, we call this family 2-*cycle-unfriendly for k'*.

Remark. In this chapter, we will say that a family is *cycle-friendly for k* meaning that the family is 2-cycle-friendly for k. The reason why we defined this term is that we will also define m-cycle-friendliness in Definition 6.16.

The MNT families for embedding degrees 4 and 6 are the only known examples of a cycle-friendly family for embedding degrees 6 and 4, respectively.

From Definition 5.6 we can see that 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). This means that there are only finitely many curves with embedding degree 4, which is in a cycle with some elliptic curve of different embedding degree 6 (and analogically for embedding degree 6). Theorem 3.6 asserts that all such cycles have both curves very small, namely $q < 64$, where q is the field size.

Lemma 5.7. Let $\mathcal{F} = (q(x), r(x), t(x))$ be a family of prime-order elliptic curves with embedding degree k that is cycle-friendly for embedding degree k'. Suppose that both $q(x)$ and $r(x)$ represent primes and are integer-valued (see Chapter 2 for definitions). Then $\mathcal{F}' = (r(x), q(x), 2 - t(x))$ is a family of prime-order elliptic curves with embedding degree k' that is cycle-friendly for k.

Proof. We will prove that $(r(x), q(x), 2 - t(x))$ satisfies all the conditions in Definition 2.3. Since both $q(x)$ and $r(x)$ represent primes and are integer-valued, we are done with the first two conditions.

We discussed that families of prime-order curves satisfy the equality $r(x) = q(x) + 1 - t(x)$, which can in turn be transformed into the desired equality $q(x) = r(x) + 1 - (2 - t(x))$.

The condition (d) comes from the fact that $\mathcal{F}$ is cycle-friendly for k' and therefore, k' is minimal such that $q(x) \mid \Phi_{k'}((2 - t(x)) - 1)$.

For the last, we need to prove that the equation

$$Dy^2 = (2 - t(x))^2 - 4r(x)$$

has infinitely many solutions (x, y). Since $\mathcal{F}$ is a family, we know that $Dy^2 = t(x)^2 - 4q(x)$ has infinitely many solutions (x, y). But $r(x) = q(x) + 1 - t(x)$ and therefore, the last condition is also satisfied.

We need to show that $\mathcal{F}'$ is cycle-friendly for k. But this is immediate since $\mathcal{F}$ is a family and therefore, k is minimal such that

$$r(x) \mid \Phi_k(t(x) - 1).$$

□

On the other hand, as we will see below, there is no k' for which the MNT3, Freeman and Barreto-Naehrig families are cycle-friendly. Before proving that, we state a lemma.

Lemma 5.8. (Lemma 5.1 in [11]) Let $f(x)$ be a polynomial with rational coefficients, 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.

The proof of this lemma is short and easy with the knowledge of Galois theory but is beyond the scope of our text. It can be found in [11] or [14].

The immediate corollary for the previous lemma is crucial for determining the embedding degree, for which a family can be cycle-friendly.

Corollary 5.9. Let $(q(x), r(x), t(x))$ be family of prime-order elliptic curves that is cycle-friendly for k. Then $\varphi(k)$ divides $\deg q(x)$.

Proof. Let $q(x), r(x)$ and $t(x)$ are the polynomials representing the family. We must check for which k's it can happen that

$$q(x) \mid \Phi_k(1 - t(x)).$$

By Lemma 5.8 we see that $\varphi(k) \mid \deg q(x)$. □

Corollary 5.9 gives us an easy algorithm to check whether a given family is cycle-friendly for some embedding degree. In the following text, let us investigate MNT3, Freeman and BN families.

Proposition 5.10. MNT3 family is 2-cycle-unfriendly for all embedding degrees.

Proof. Recall the MNT3 family.

$$\begin{aligned} q(x) &= 12x^2 - 1 \\ r(x) &= 12x^2 - 6x + 1 \\ t(x) &= 6x - 1 \end{aligned}$$

By Corollary 5.9 we see that $\varphi(k)$ is 2 (recall that $\varphi(k) = 2$, implying $k \in \{1, 2\}$ is impossible by the discussion in Chapter 3). This means that k is 3, 4 or 6, but Proposition 3.7 asserts that none of these is possible. □

Proposition 5.11. Freeman family is 2-cycle-unfriendly for all embedding degrees.

Proof. Recall that the Freeman family is represented by polynomials

$$\begin{aligned} q(x) &= 25x^4 + 25x^3 + 25x^2 + 10x + 3, \\ r(x) &= 25x^4 + 25x^3 + 15x^2 + 5x + 1, \\ t(x) &= 10x^2 + 5x + 3. \end{aligned}$$

Suppose that Freeman family is cycle friendly for k. Then by Corollary 5.9, $\varphi(k) \mid 4$ and short calculation shows that this can happen only for $k \in \{1, 2, 3, 4, 5, 6, 8, 10, 12\}$. Recall from Chapter 3 that it cannot happen that $k \in \{1, 2\}$.

We are searching for suitable $k \in \{3, 4, 5, 6, 8, 10, 12\}$ such that

$$q(x) \mid \Phi_k(1 - t(x)).$$

If the Freeman family were cycle-friendly for $k = 3, 4$, or 6, then the respective MNT family would have to be cycle-friendly for the Freeman family, but that is not true (MNT4 and MNT6 are cycle-friendly for each other, and MNT3 is cycle unfriendly for all embedding degrees).

We then used computational tools to show that there are in fact no embedding degrees for which the Freeman family is cycle-friendly. Using Sage[16], we see that $\Phi_k(1 - t(x))$ is irreducible of degree 8 for $k = 8, 10, 12$ and $\Phi_5(1 - t(x))$ is

$$(400x^4 + 400x^3 + 240x^2 + 60x + 11)(25x^4 + 25x^3 + 15x^2 + 5x + 1).$$

□

A very similar argument also works for the Barreto-Naehrig family representing prime-order elliptic curves with embedding degree 12.

16. Implementation can be found in the file `cycle_friendliness.py` in the attachment as the function `is_Freeman_cycle_friendly()`.

Proposition 5.12. Barreto-Naehrig family is 2-cycle-unfriendly for all embedding degrees.

Proof. Recall that the BN family is the triple of polynomials

$$\begin{aligned} q(x) &= 36x^4 + 36x^3 + 24x^2 + 6x + 1, \\ r(x) &= 36x^4 + 36x^3 + 18x^2 + 6x + 1, \\ t(x) &= 6x^2 + 1. \end{aligned}$$

Following the previous proof, we only need to check if there is some k such that

$$q(x) \mid \Phi_k(1 - t(x))$$

holds. Similarly as above, by Corollary 5.9 we can see that k must be $3, 4, 5, 6, 8, 10$, or 12, but again, this cannot happen for $3, 4, 6$ and using Sage[17] we see that $\Phi_k(1 - t(x))$ is irreducible of degree 8 for $k = 5, 8, 10$ and $\Phi_{12}(1 - t(x))$ is

$$(36x^4 + 36x^3 + 18x^2 + 6x + 1)(36x^4 - 36x^3 + 18x^2 - 6x + 1).$$

□

Although none of the previous families is cycle-friendly, there still may be cycles containing curves in these families. We used a simple brute-force calculation (Algorithm 3, ran in PARI-GP and Sage) for determining if there is some l such that $q(l) \mid \Phi_k(1 - t(l))$ for some small values of k and found that:

- there is only one cycle of type $(3, 10)$, namely $q_1 = 11, q_2 = 7$. There are no other cycles of type $(3, k)$ for any $k = 1, \ldots, 22$.
- there are no cycles of type (FR, k) for any $k = 1, \ldots, 22$.
- there is only one cycle of type $(12, 18)$ where the first is in BN family, namely $q_1 = 19$ and $q_2 = 13$. Except this cycle, there are no other cycles of type (BN, k) for any $k = 1, \ldots, 36$.

In particular, we have the following answer for 2-cycles to one of the open problems mentioned in [7].

17. Implementation can be found in the file `cycle_friendliness.py` in the attachment as the function `is_BN_cycle_friendly()`.

Corollary 5.13. There are no 2-cycles from combinations of MNT, BN and Freeman curves, other than cycles of type $(4, 6)$. [18]

This result also partially answers the discussion given on the blog of Michael Straka[19].

5.2 Lower bounds on the embedding degree

A further search could be helpful to find more cycles, which contain a curve in the mentioned families. Although, by Lemma 5.3 we know that there are only finitely many values l such that $q(l) \mid \Phi_k(1 - t(l))$. Therefore, we have an upper bound on $|l|$, which means that we have an upper bound on $q(l)$, the field size of a curve in the cycle.

Theorem 5.14. Let $\mathcal{F} = (q(x), r(x), t(x))$ be a family of prime-order elliptic curves with embedding degree k and let k' be an integer such that the family $\mathcal{F}$ is cycle-unfriendly for embedding degree k'. There is an efficiently computable upper bound Q (depending only on $\mathcal{F}$ and k) such that for any $l \in \mathbb{Z}$ for which the elliptic curve specified by $q = q(l), r = r(l)$ lies in a cycle of type $(\mathcal{F}, k')$, it holds that $q(l) \leq Q$.

Furthermore, let $\Phi_{k'}(1 - t(x)) = f(x)q(x) + g(x)$ for some polynomials $f(x), g(x)$ with $\deg g(x) < \deg q(x)$. The bound Q can be set to $\max\{q(l) \mid |l| \leq |m|\}$, where m is the largest real root (in absolute value) of the polynomial

$$M(x) = (q(x) - g(x))(q(x) + g(x)).$$

Proof. The first part is an immediate corollary of Lemma 5.3.

For the second part, we need to prove that for any l, for which $q(l) \mid g(l)$, it holds that $q(l) \leq q(m) = \pm g(m)$, where m is defined as in the theorem.

The polynomial $M(x)$ is an even-degree polynomial of degree $\deg M(x) = 2 \deg q(x)$, since $\deg g(x) < \deg q(x)$. Therefore,

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

18. We should mention that the second curve in the $(3, 10)$ cycle is not in the Freeman family.

19. Available on `https://www.michaelstraka.com/posts/recursivesnarks/`.

It follows that for any $\alpha \in \mathbb{R}$ such that $M(\alpha) \leq 0$ it must hold that $|\alpha| \leq |m|$.

Let $l \in \mathbb{Z}$ be an integer such that $q(l) \mid g(l)$. Then $|q(l)| \leq |g(l)|$ and therefore, $0 \geq q(l)^2 - g(l)^2 = M(l)$. As discussed before, this means that $|l| \leq |m|$. Therefore, $q(l) \leq Q$ (as defined in the theorem). □

Table 5.1: Lower bounds on embedding degrees

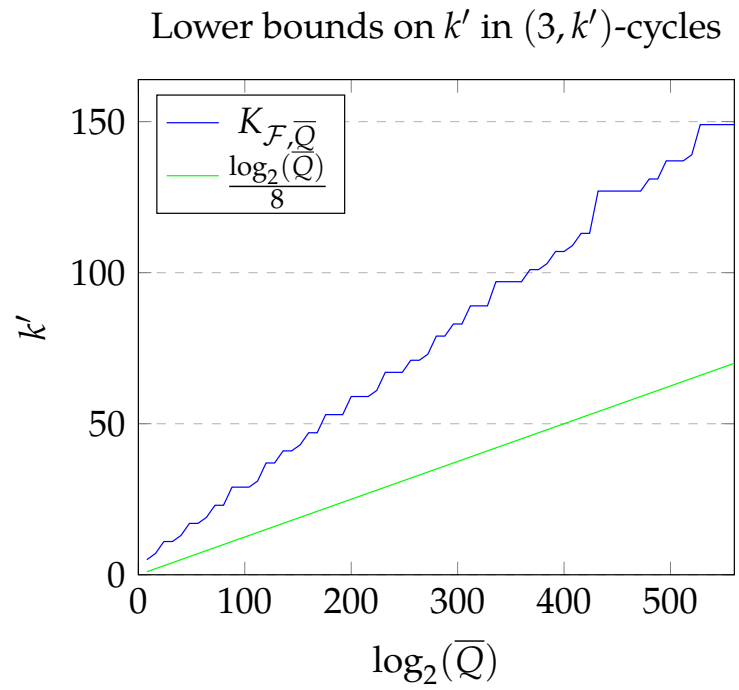
$\log_2(q)$	128	192	256	384	512
Pairing-friendly	16	24	32	48	64
MNT3	37	53	71	103	137
Freeman	23	29	41	59	73
BN	29	43	59	83	109

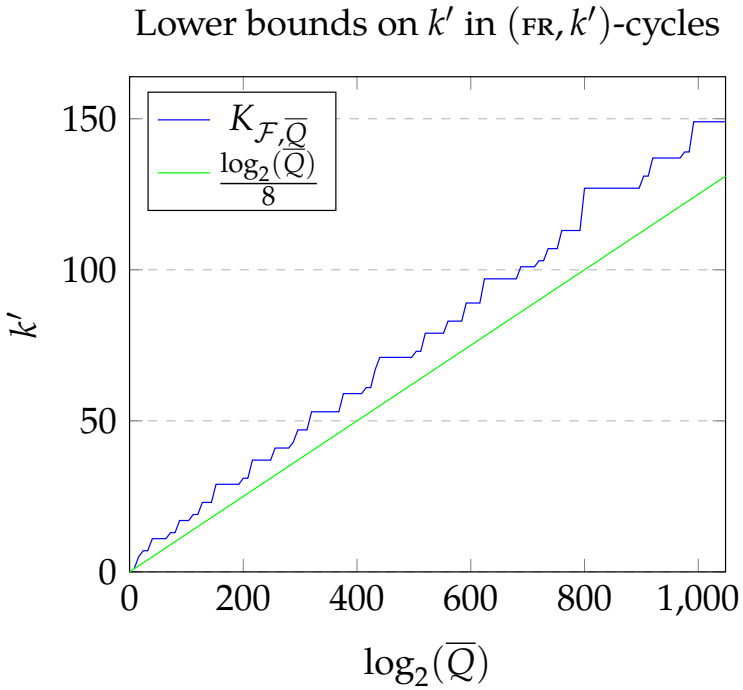
We see that given k', there is an upper bound on q. Therefore, if we have a lower bound $\overline{Q}$ on q, we can look at the first k (if such exists), for which the upper bound on q is at least $\overline{Q}$. In particular, we have the following corollary.

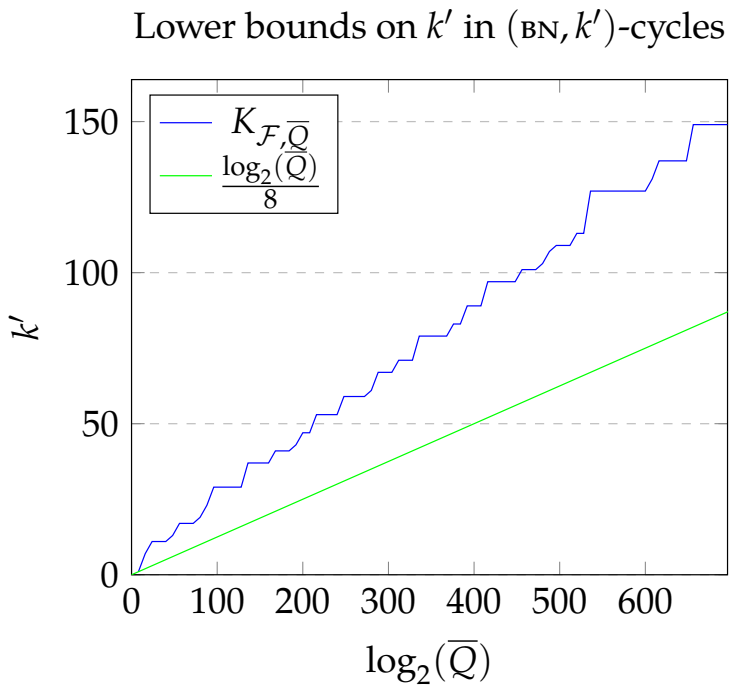
Corollary 5.15. Let $\mathcal{F}$ be a family of elliptic curves, and $\overline{Q}$ be a lower bound on field sizes of curves in $\mathcal{F}$. There is an efficiently computable lower bound K, depending only on $\mathcal{F}$ and $\overline{Q}$, for which any cycle of type $(\mathcal{F}, k')$ must satisfy $k' \leq K$.

Definition 5.16. Given family $\mathcal{F}$ and the second embedding degree k', we denote the upper bound Q defined in Theorem 5.14 as $Q_{\mathcal{F},k'}$ and the lower bound K from the corollary as $K_{\mathcal{F},\overline{Q}}$.

We computed the lower bounds $K_{\mathcal{F},\overline{Q}}$ for our families (MNT3, Freeman, BN) for small bit sizes of q (namely up to the highest q such that the minimal k' is less than an arbitrarily chosen value of 150; so as the computation finishes in reasonable time). In the following, we provide an overview of the results. We mention the algorithms we used in Section 5.4. For completeness, we mention cryptographically interesting values of $\log_2(q)$ explicitly in Table 5.1.


Lower bounds on k' in $(3, k')$-cycles
$K_{\mathcal{F},\overline{Q}}$
$\frac{\log_2(\overline{Q})}{8}$
150
100
50
0
k'
0
100
200
300
400
500
$\log_2(\overline{Q})$


Lower bounds on k' in (FR, k')-cycles
$K_{\mathcal{F},\overline{Q}}$
$\frac{\log_2(\overline{Q})}{8}$
150
100
50
0
k'
0
200
400
600
800
1,000
$\log_2(\overline{Q})$



It seems reasonable to us to conjecture that this "linear" trend in the lower bounds on k' will continue, leading to an interesting result.

Conjecture 5.17. There are no pairing-friendly (in the sense of Definition 1.16) 2-cycles containing a curve in the BN or Freeman families.

Since the function $K_{\mathcal{F},\overline{Q}}(\log_2(\overline{Q}))$ is non-decreasing, our computation proves this conjecture for the field sizes up to 2^{1200}, since we computed this for $K_{\mathcal{F},\overline{Q}} \leq 150$ and $\frac{\log_2(q)}{8} \geq 150$ for $q \geq 2^{1200}$.

In the case of the MNT3 family, we found an argument stating that (informally speaking) "the green line continues to be a lower bound on k'", implying that there are *no pairing-friendly 2-cycles* containing a curve in the MNT3 family. This argument is presented in the following section.

5.3 A solution to the conjecture in the case of MNT3

In this section, we prove the following result.

Proposition 5.18. There are no pairing-friendly (in the sense of Definition 1.16) 2-cycles containing a curve with embedding degree 3.

We will need the following result, known as the *Upper and Lower Bound Theorem*. We will state only the "Upper Bound" part.

Theorem 5.19 (Upper Bound Theorem[20])**.** Let $f(x)$ be a polynomial with real coefficients and positive leading coefficient, and let $a \geq 0$ be a real number. Using long division of polynomials, write $f(x) = (x-a)q(x) + r$. If both $q(x)$ and r have only positive coefficients, then a is the upper bound on real zeroes of the polynomial $f(x)$.

Proof. [21] Let $a \geq 0$ be a real number such that $q(x)$ and r have only positive coefficients. We will prove that given any real $c > a$, $f(c) \neq 0$, which will finish the proof.

Let us factor $(x-a)$ from the right hand side of the long division, we obtain

$$f(x) = (x-a)\Big(q(x) + \frac{r}{x-a}\Big).$$

Therefore, we can write $f(c) = (c-a)(q(c) + \frac{r}{c-a})$. Since $c > a$, $c - a > 0$. Since $q(x)$ has only positive coefficients and $c > a \geq 0$, $q(c) > 0$. Similarly, $r > 0$, $(c-a) > 0$ and therefore $\frac{r}{c-a} > 0$. Hence, $f(c) > 0$. □

The following lemma is very long and technical. We recommend the reader to accept the bounds given in the lemma as a fact and skip to Corollary 5.21 at first sight.

20. This is *not* the Upper Bound Theorem from combinatorics.
21. The proof is inspired by the discussion at `https://math.stackexchange.com/questions/1633846/proof-for-theorem-of-upper-and-lower-bounds-on-zeroes-of-polynomials`

Lemma 5.20. 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 1.13, 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.

$$\alpha^k - 1 = \Pi_k^+ \cdot (a_k\alpha + b_k) \tag{5.1}$$

$$\beta^k - 1 = \Pi_k^- \cdot (a_k\beta + b_k) \tag{5.2}$$

Using (5.2), we express b_k in terms of β, k, Π_k^- and a_k, and plugging into (5.1) we obtain formula for a_k. Similarly, we also get a formula for b_k.

$$a_k = \frac{\Pi_k^-(\alpha^k - 1) - \Pi_k^+(\beta^k - 1)}{\Pi_k^+\Pi_k^-(\alpha - \beta)} \tag{5.3}$$

$$b_k = \frac{\alpha\Pi_k^+(\beta^k - 1) - \beta\Pi_k^-(\alpha^k - 1)}{\Pi_k^+\Pi_k^-(\alpha - \beta)} \tag{5.4}$$

Let us denote

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

A simple computation shows that

$$a_k = \frac{u_k - v_k}{2\sqrt{3}}, \qquad b_k = \frac{u_k + v_k}{2} - 2a_k. \tag{5.5}$$

By the definition of the cyclotomic polynomial (Definition 1.11),

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

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

Since $|\zeta_k| = 1$,

$$|2 - \sqrt{3} - \zeta_k^i| \le 3 - \sqrt{3},$$
$$|2 + \sqrt{3} - \zeta_k^i| \ge 1 + \sqrt{3}.$$

Therefore,

$$\left|\frac{v_k}{u_k}\right| \le \left(\frac{3 - \sqrt{3}}{1 + \sqrt{3}}\right)^{\varphi(k)} = (2\sqrt{3} - 3)^{\varphi(k)}. \tag{5.6}$$

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,

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

But we know that $\frac{v_k}{u_k} \le (2\sqrt{3} - 3)^{\varphi(k)} \le (2\sqrt{3} - 3)^2 < 1$, implying $u_k > v_k$. This proves part a).

We will divide (b) into three parts.

- Now we will prove that $2a_k + b_k > 0$. By (5.3) and (5.4), a short calculation shows

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

But from (5.1) and (5.2) 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 $b_k \leq a_k$, or equivalently, $\frac{b_k}{a_k} \leq 1$ since a_k is positive. Using (5.5), 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 $\frac{1+\frac{v_k}{u_k}}{1-\frac{v_k}{u_k}} \leq \sqrt{3}$ in several steps:

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

The equality holds since $u_k > 0$ and $v_k > 0$. The first inequality holds from (5.6) 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 $\varphi(k) \geq 2$. The last inequality is an easy computation.

- The only remaining inequality is $a_k < 4^k$. Note that by (5.3),

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

  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). Therefore, $\Pi_k^- < 0$.

  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.

□

Corollary 5.21. 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 $0 < B_k \leq -\frac{A_k}{2}$.

Proof. Let $z = -6x+2$. Then $3(12x^2-1) = z^2 - 4z + 1$ and the long division used in the statement of Lemma 5.20 becomes

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

Therefore, $A_k = -6a_k$ and $B_k = 2a_k + b_k$ and the statement follows from Lemma 5.20. □

Proof of Proposition 5.18. Let $(3,k)$ be a cycle of elliptic curves. If the field size of the curve with embedding degree 3 is less than 256, Definition 1.16 asserts that $k < 1$, which is clearly impossible. In particular, the field sizes are greater than 64, so we can assume that the curve with embedding degree 3 is in the MNT3 family (see Theorem 2.4).

By Lemma 5.3,

$$q(l) \mid \Phi_k(1 - t(l)) \iff q(l) \mid A_k x + B_k,$$

where $A_k, B_k \in \mathbb{Q}$ are obtained from the long division of polynomials:

$$\Phi_k(1 - t(x)) = q(x)f(x) + A_k x + B_k,$$

and $q(x) = 12x^2 - 1$ and $t(x) = 6x - 1$ are the MNT3 polynomials.

We need to prove that for a given l, we have $k > \frac{\log_2 q(l)}{8}$ (see Definition 1.16), or equivalently, $2^{8k} > q(l)$.

Recall that by Definition 5.16. $Q_{\mathsf{mnt3},k}$ is defined as the maximum of values $q(l)$ for $|l| \leq |m|$, where m is the largest real root (in absolute value) of $M(x) = (12x^2 - A_k x - B_k - 1)(12x^2 + A_k x + B_k - 1)$. Since $q(x) = 12x^2 - 1$ is an even function, which is monotone on the intervals $(-\infty, 0]$ and $[0, \infty)$, we have $Q_{\mathsf{mnt3},k} = q(m)$.

The main idea of the prove of Proposition 5.18 is to show that $X = \sqrt{\frac{2^{8k}+1}{12}}$ is an upper bound on the roots for $M(x)$. Then, since $X > m$, it will hold that $2^{8k} = 12X^2 - 1 > 12m^2 - 1 = q(m) = Q_{\mathsf{mnt3},k}$.

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 will use the Upper Bound Theorem and apply the long division of polynomials to show that $2^{4k-2} < X$ is an upper bound on roots of both of the polynomials in (a) and (b), respectively.

(a) We can write $12x^2 - A_k x - B_k - 1 = (x - 2^{4k-2})f(x) + g$, where

$$f(x) = 12x + 12 \cdot 2^{4k-2} - A_k,$$

$$g = 12 \cdot 2^{8k-4} - 2^{4k-2}A_k - B_k - 1.$$

We want to prove that

$$12 \cdot 2^{4k-2} - A_k > 0,$$

$$12 \cdot 2^{8k-4} - 2^{4k-2}A_k > B_k + 1.$$

But both inequalities follow easily from Corollary 5.21. The first inequality comes directly from $A_k < 0$, and for the second, we will use $-A_k \geq 2B_k$.

$$12 \cdot 2^{8k-4} - 2^{4k-2}A_k \geq 12 \cdot 2^{8k-4} + 2^{4k-1}B_k > B_k + 1$$

(b) We can write $12x^2 + A_k x + B_k - 1 = (x - 2^{4k-2})f(x) + g$, where

$$f(x) = 12x + 12 \cdot 2^{4k-2} + A_k,$$

$$g = 12 \cdot 2^{8k-4} + 2^{4k-2}A_k + B_k - 1.$$

We want to prove that

$$12 \cdot 2^{4k-2} + A_k > 0,$$

$$12 \cdot 2^{8k-4} + 2^{4k-2}A_k > -B_k + 1.$$

We will again use the Corollary 5.21. The first inequality comes from $-6 \cdot 2^{2k} < A_k$ and the second comes from the same fact and from $B_k \leq 1$.

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

Therefore, we found that 2^{4k-2} is a strict upper bound on the real roots of the polynomial $M(x)$, and hence $2^{8k} > 12(2^{4k-2})^2 - 1 = Q_{\mathsf{mnt3},k'}$, which proves Proposition 5.18. □

5.4 Algorithms used in this chapter

In this section, we give a sketch of the algorithms we used. The mentioned algorithms are implemented in the file `algorithms.py` in the attachment.

Algorithm 2 is based on the *Upper and Lower Bounds Theorem*, which we presented in the previous section as Theorem 5.19. To get a lower bound on zeroes of $f(x)$, we find an upper bound on zeroes of $f(-x)$ and switch the sign.

Remark. When generating graphs on pages 46 and 47, we optimized Algorithm 4. If we want to compute smallest_k for multiple values of bits, we can compute the values m only once, save it and then check the smallest k's.[22]

22. This is implemented as the function `graph_smallest_k(qx, tx, max_k)` in the file `algorithms.py`.

Algorithm 2: upper_bound($f(x)$)

$i \leftarrow 1$
while *1* **do**
  guess $\leftarrow 2^i$
  Write $f(x) = (x - \text{guess}) \cdot g(x) + h$ using long division of polynomials.
  if *Both $g(x)$ and h have only positive coefficients* **then**
    break
Use binary search to find the largest root r of $f(x)$, since $\frac{\text{guess}}{2} \leq r \leq \text{guess}$
return r

Algorithm 3: find_cycles($q(x), t(x)$, max_k=100)

$r(x) \leftarrow q(x) + 1 - t(x)$
for $k \leftarrow 1 \ldots max\_k$ **do**
  Write $\Phi_k(1 - t(x)) = q(x)f(x) + g(x)$ using long division
  $l \leftarrow \min(\text{lower\_bound}(q(x) - g(x)), \text{lower\_bound}(q(x) + g(x)))$
  $u \leftarrow \max(\text{upper\_bound}(q(x) - g(x)), \text{upper\_bound}(q(x) + g(x)))$
  for $i \leftarrow l \ldots u$ **do**
    if $q(i) \mid g(i)$ & $q(i)$ *is a prime* & $r(i)$ *is a prime* **then**
      There is a 2-cycle where first curve is in the family and represented by $q = q(i)$ and $r = r(i)$ and the second curve has embedding degree k.

Algorithm 4: smallest_k(bits, $q(x)$, $t(x)$, max_k=100)

for $k \leftarrow 1 \ldots max\_k$ **do**
  Write $\Phi_k(1 - t(x)) = q(x) \cdot f(x) + g(x)$ for $\deg g(x) < \deg q(x)$.
  $l \leftarrow \min(\text{lower\_bound}(q(x) - g(x)), \text{lower\_bound}(q(x) + g(x)))$
  $u \leftarrow \max(\text{upper\_bound}(q(x) - g(x)), \text{upper\_bound}(q(x) + g(x)))$
  $m \leftarrow \max(-l, u)$
  if $q(m) \geq 2^{bits}$ **then**
    return k
return *The lower bound on k is greater than max_k.*

6 Further topics

In this chapter, we summarise our results, partial results and open questions, which showed up during our study of elliptic curve cycles, and which we believe may be an interesting direction to study in the future.

6.1 The conjecture in the case of arbitrary families

At the beginning of the proof of Proposition 5.18, there was nothing special about the polynomials and numbers that showed up. We will sketch a possible proof of the conjecture for *any family of prime-order elliptic curves* $\mathcal{F} = (q(x), r(x), t(x))$. Let n denote the degree of $q(x)$. Let us perform the long division of polynomials.

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

Now, notice that

$$(1 - t(x))^k - 1 = \prod_{d|k} \Phi_k(1 - t(x))$$

and reducing this by $q(x)$ we obtain

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

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

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

Then we have the following system of equations.

$$\begin{aligned}
(1 - t(\alpha_1))^k - 1 &= \Pi_{k,\alpha_1} \cdot (A_{k,n-1}\alpha_1^{n-1} + \ldots + A_{k,1}\alpha_1 + A_{k,0}) \\
&\vdots \\
(1 - t(\alpha_n))^k - 1 &= \Pi_{k,\alpha_n} \cdot (A_{k,n-1}\alpha_n^{n-1} + \ldots + A_{k,1}\alpha_n + A_{k,0})
\end{aligned}$$

Since the system is linear for n variables $A_{k,0} \dots A_{k,n-1}$ and we have n equations (not linearly dependent), we are able to write down the formulas for $A_{k,i}$. Therefore, it should be possible to state some bounds on $A_{k,i}$, which could help us to prove that $2^{8k} > Q_{\mathcal{F},k}$ (as in Proposition 5.18).

Nevertheless, such proof would be much longer and much more technical than the proof of Proposition 5.18. It would be much better to find a more straightforward argument; we leave this as an open problem.

6.2 Further search of $(3, k)$-cycles

When proving Proposition 5.18, we have found very interesting behaviour of the remainder in the long division of the cyclotomic polynomial by $x^2 - 4x + 1$.

Proposition 6.1. Let $k > 2$ and let

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

Then $\lim_{k\to\infty} \frac{a_k}{b_k} = -(2 + \sqrt{3})$.

Proof. We will use the same notation as in the proof of Lemma 5.20.

$$a_k = \frac{u_k - v_k}{2\sqrt{3}}$$

$$b_k = \frac{u_k + v_k}{2} - 2a_k$$

Recall that $|\frac{v_k}{u_k}| \leq (2\sqrt{3} - 3)^{\varphi(k)}$. Because $\lim_{k\to\infty} \varphi(k) = \infty$, we get that $\lim_{k\to\infty} |\frac{v_k}{u_k}| = 0$ (since $0 < 2\sqrt{3} - 3 < 1$). Then

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

$$\lim_{k\to\infty} \frac{a_k}{b_k} = \frac{1}{-2 + \sqrt{3}} = -(2 + \sqrt{3}).$$

□

Corollary 6.2. Let $k > 2$ and let

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

Then $\lim_{k\to\infty} \frac{A_k}{B_k} = -\sqrt{12}$.

Proof. Recall the substitution $A_k = -6a_k$ and $B_k = 2a_k + b_k$. A straightforward computation shows the statement.

$$\lim_{k\to\infty} \frac{A_k}{B_k} = \lim_{k\to\infty} \frac{-6a_k}{2a_k + b_k} = \lim_{k\to\infty} \frac{-6\frac{a_k}{b_k}}{1 + 2\frac{a_k}{b_k}} = \frac{6(2+\sqrt{3})}{1-2(2+\sqrt{3})} = -\sqrt{12}.$$

□

We tried to investigate, for which x it holds that $12x^2 - 1 \mid A_k x + B_k$. For such x there must exist d such that

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

so $12dx^2 - A_k x - B_k - d = 0$ must have an integer solution. The discriminant of the polynomial must be a square

$$y^2 = A_k^2 + 48dB_k + 48d^2,$$

and this equation ($48d^2 + 48B_k d + A_k^2 - y^2 = 0$) must have an integer solution for d. The discriminant is

$$8^2(36B_k^2 - 3A_k^2 + 3y^2)$$

Thus, if there is an elliptic curve of embedding degree 3 in a cycle with a curve of embedding degree k, then there exists y such that $36B_k^2 - 3A_k^2 + 3y^2$ is a square and then the corresponding d is an integer. Then we observed (but did not prove) the following.

Conjecture 6.3. Let $k > 2$ and let

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

Then the following is true.

(a) $36B_k^2 - 3A_k^2 = z^2$ for suitable $z \in \mathbb{Z}$, and for all primes $p > k$ dividing z it holds that

- p^2 does not divide z
- $p \equiv \pm 1 \pmod{k}$.

(b) $B_k^2 - 3(\frac{A_k}{6})^2$ divides B_k^2. Furthermore, if $\varphi(k)$ is not divisible by 4, $4(B_k^2 - 3(\frac{A_k}{6})^2)$ divides B_k^2.

Even if we have answers to these questions, it does not seem to help us characterize the embedding degrees in $(3, k)$-cycles. As an example of the behaviour, we show two examples; the smallest embedding degrees in $(3, k)$-cycles are 10 and 23 (both have very small field sizes).

For $k = 10$, the polynomial $A_k x + B_k$ is $-264x + 77$, $d = -17, y = 144$ and

$$36B_k^2 - 3A_k^2 = 66^2$$

$$66^2 + 3 \cdot y^2 = 258^2$$

For $k = 23$, the polynomial $A_k x + B_k$ is

$$-9054520347606 \cdot x + 2613814880038,$$

The values $d = -329685655642, y = 6770391123210 \neq f^2$ for any $f \in \mathbb{Z}$, and

$$36B_k^2 - 3A_k^2 = 16033674^2$$

$$16033674^2 + 3 \cdot y^2 = 11726661412524^2$$

6.3 Cycles of type (k, k)

We have also widely investigated if there are some cycles of type (k, k) for some positive integer k. As mentioned in Section 3.2, the values $k = 1, 2, 3, 4, 6, 8, 12$ are out of the game for multiple reasons. In this section, we present some partial results about these cycles.

In order to find some 2-cycles with the same embedding degrees, we investigated a bit more general problem: which prime numbers q_1, q_2 satisfy, that q_1 has the same multiplicative order modulo q_2 as q_2 modulo q_1? Note that this is the same problem as searching for a

(k, k)-cycle, where k is the multiplicative order, only without the Hasse condition. It turns out that such prime numbers (q_1, q_2) exist and *they can be surprisingly close to each other* [23], for example $(5, 13)$ with order 4, $(67, 89)$ with order 11, or $(241, 281)$ with order 20. Although, none of these satisfies the Hasse condition. The following definition brings a notion of "closeness" in the sense of the Hasse bound.

Definition 6.4. Let q_1, q_2 be prime numbers. Denote the value $\frac{q_2 - q_1 - 1}{\sqrt{q_1}}$ as $d(q_1, q_2)$.

The following lemma says that for a pair of prime numbers, to be field sizes for a cycle of elliptic curves, the value $d(q_1, q_2)$ must be less or equal to 2 (this is precisely the Hasse bound).

Lemma 6.5. Let q_1, q_2 be prime numbers. Then q_2 is in the Hasse interval of q_1 if and only if $|d(q_1, q_2)| \leq 2$.

Proof. Let $q_1 < q_2$ be prime numbers. The following are equivalent.

$$q_1 + 1 - 2\sqrt{q_1} \leq q_2 \leq q_1 + 1 + 2\sqrt{q_1},$$

$$-2 \leq \frac{q_2 - q_1 - 1}{\sqrt{q_1}} \leq 2.$$

But the first line says precisely that q_1 is in the Hasse interval of q_2 and the second line says that $|d(q_1, q_2)| \leq 2$. □

Recall that Proposition 3.1 asserts that "being in the Hasse interval of" is a symmetric relation. As a corollary, we have the following result.

Corollary 6.6. Let q_1, q_2 be prime numbers. Then $|d(q_1, q_2)| \leq 2$ if and only if $|d(q_2, q_1)| \leq 2$.

We have also found the following computational result:

Proposition 6.7. There are only two prime number pairs (q_1, q_2) for $q_1 < 10^6$ and $q_1 < q_2$, such that the multiplicative order of q_1 modulo q_2 is the same as the order of q_2 modulo q_1, and $d(q_1, q_2) \leq 3$ (equivalently, $q_2 \leq q_1 + 1 + 3\sqrt{q_1}$). Those are $(67, 89)$ and $(241, 281)$ and

$$2.5 < d(q_1, q_2) < 2.6$$

in both cases.

23. Note that $(q_1, q_2) = (7, 13), (73, 89)$, or $(251, 281)$ satisfy the Hasse condition.

This leads us to the following. If we want to prove that there are no (k,k)-cycles, we cannot omit the Hasse bound. This was unnecessary in the cases of $(1,1)$-cycles and $(2,2)$-cycles, simply because the ideas used in the proof hold in general for all prime number pairs.

6.3.1 Proof of the proven

We now prove a result that has been proven before (in Corollary 3.8). Note that our proof does not use the fact that any elliptic curve with embedding degree 4 is represented by some polynomials (see Theorem 2.4). It might be interesting to generalize this idea for other values of k.

Proposition 6.8. There are no cycles of type $(4,4)$.

Proof. Let $q_1 < q_2$ be prime numbers such that they form a cycle of type $(4,4)$. The condition given in Lemma 1.14 becomes

$$q_1 \mid q_2^2 + 1$$

$$q_2 \mid q_1^2 + 1$$

Let us write $q_2^2 + 1 = q_1 \cdot k$ a $q_1^2 + 1 = q_2 \cdot l$ for suitable k, l. Subtracting the equations we get

$$\begin{aligned} q_2^2 - q_1^2 &= q_1 \cdot k - q_2 \cdot l \\ q_1(q_1 + k) &= q_2(q_2 + l) \end{aligned}$$

Denote $n = \gcd(q_1 + k, l + q_2)$. Then

$$\begin{aligned} q_2 + l &= q_1 \cdot n \\ q_1 + k &= q_2 \cdot n \end{aligned} \tag{6.1}$$

We now prove that $n \geq 3$. Clearly $n \neq 1$, because then it would hold $q_2 + l = q_1$ a $q_1 + k = q_2$, but $q_1, q_2, k, l > 0$, contradiction. Because $q_1 k = q_2^2 + 1$ is even, k must be even, thus $q_1 + k$ is odd, hence $\gcd(q_1 + k, q_2 + l) = n$ is odd.

The equation 6.1 says that $q_2 + k > q_1 + k = q_2 n \geq 3q_2$, so $k > 2q_2$.

If $q_1 \geq 5$, it holds

$$\begin{aligned} q_1^2 &> 4q_1 + 1 \\ q_1^2 + 1 &> 4q_1 + 2 \\ q_2 l &> 4q_1 + 2 \\ q_2 l + q_1 k - q_1 k &> 4q_1 + 2 \\ q_2 l + q_1 k - 2q_1 q_2 &> 4q_1 + 2 \\ q_1^2 + 1 + q_2^2 + 1 - 2q_1 q_2 &> 4q_1 + 2 \\ q_1^2 + q_2^2 - 2q_1 q_2 &> 4q_1 \\ (q_2 - q_1)^2 &> 4q_1 \\ q_2 - q_1 &> 2\sqrt{q_1} \text{ (Both sides are positive)} \end{aligned}$$

If $q_1 < 5$, we check all the possibilities and find out that there are no $(4,4)$-cycles. □

A very similar argument can be used for cycles of type $(3,3)$ and possibly for type $(6,6)$, but unfortunately, it does not seem to extend to a general case. Intuitively, this is because $\varphi(k) = 2$ for $k = 3, 4$ or 6, and therefore, "the squares in the condition $q_1 \mid \Phi_k(q_2)$ fit nicely with the square root in the Hasse bound". For other values of k, this does not seem to happen.

6.3.2 Splitting of the field sizes of (k,k)-cycles in k-th cyclotomic field

This section is beyond the scope of our text, and the reader can freely skip to the following section without any loss of the flow of the text. We try to understand if it is possible to have a cycle of type (k,k) for an arbitrarily chosen value k. We found complete factorization of the ideals (q_1) and (q_2), in fact, these ideals split completely in $\mathbb{Q}(\zeta_k)$ (the k-th cyclotomic field). Our idea for an improvement is that when k is "small", the factors of the ideals are principal, and it could be interesting to study this case (since we are aiming for small k).

Let us begin with two well-known theorems from algebraic number theory.

Theorem 6.9. (Theorem 5.9. in [9]) Let $K \subseteq L$ be a Galois extension, and let $\mathfrak{p}$ be prime in K.

(a) The Galois group $\mathrm{Gal}(L/K)$ acts transitively on the primes of L containing $\mathfrak{p}$, i.e., if $\mathfrak{P}$ and $\mathfrak{P}'$ are primes of L containing $\mathfrak{p}$, then there is a $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\mathfrak{P}) = \mathfrak{P}'$.

(b) The primes $\mathfrak{P}_1, \ldots \mathfrak{P}_g$ of L containing $\mathfrak{p}$ all have the same ramification index e and the same inertial degree f, so $efg = [L : K]$.

Theorem 6.10. (Proposition 5.11. in [9]) Let $K \subseteq L$ be a Galois extension, where $L = K(\alpha)$ for some $\alpha \in \mathcal{O}_L$. Let $f(x)$ be the monic minimal polynomial of α over K, so that $f(x) \in \mathcal{O}_K[x]$. If $\mathfrak{p}$ is a prime in $\mathcal{O}_K$ and $f(x)$ is separable modulo $\mathfrak{p}$, then

(a) $\mathfrak{p}$ is unramified in L

(b) If $f(x) \cong f_1(x) \ldots f_g(x) \pmod{\mathfrak{p}}$, where $f_i(x)$ are distinct and irreducible modulo $\mathfrak{p}$, then $\mathfrak{P}_i = \mathfrak{p}\mathcal{O}_L + f_i(\alpha)\mathcal{O}_L$ is a prime ideal of $\mathcal{O}_L$, $\mathfrak{P}_i \neq \mathfrak{P}_j$ for $i \neq j$, and

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \ldots \mathfrak{P}_g.$$

Furthermore, the $f_i(x)$ all have the same degree, which is equal to the inertial degree f.

(c) $\mathfrak{p}$ splits completely in L if and only if $f(x) \equiv 0 \pmod{\mathfrak{p}}$ has a solution in $\mathcal{O}_K$.

Suppose that $q_1 \mid \Phi_k(q_2)$, thus there is a solution for $\Phi_k(x) \equiv 0 \pmod{q_1}$ in $\mathbb{Z}$. By Theorem 6.10, $q_1\mathbb{Z}[\zeta_k]$ splits completely in $\mathbb{Q}(\zeta_k)$, so $q_1\mathbb{Z}[\zeta_k] = \mathfrak{P}_1 \ldots \mathfrak{P}_{\varphi(k)}$, where $\mathfrak{P}_i$ are prime ideals of $\mathbb{Z}[\zeta_k]$ and $\mathfrak{P}_i = (q_1, f_i(\zeta_k))$, where $f_i(x)$ are irreducible factors of $\Phi_k(x)$. We do not know the precise factorization of the polynomial $\Phi_k(x)$, but we know one irreducible factor, which is $(x - q_2)$. Hence one of $\mathfrak{P}_i$'s, say $\mathfrak{P}_1$, is $(q_1, \zeta_k - q_2)$. Now we can use Theorem 6.9 and apply all automorphisms $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ on this prime ideal and we achieve all primes dividing $q_1\mathbb{Z}[\zeta_k]$, thus we achieve the prime factorization. The Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_k)/\mathbb{Q})$ consists of automorphisms sending $\zeta_k \mapsto \zeta_k^m$ for $m < k$ prime to k, thus the prime factorization is

$$q_1\mathbb{Z}[\zeta_k] = \prod_{1 \leq m < k, (m,k)=1} (q_1, \zeta_k^m - q_2).$$

Similarly,

$$q_2\mathbb{Z}[\zeta_k] = \prod_{1\leq m<k,(m,k)=1} (q_2, \zeta_k^m - q_1).$$

Furthermore, each $(p, \zeta_k^m - q)$ have norm p.
Thus, we have the following proposition.

Proposition 6.11. Let q_1, q_2 be prime numbers representing prime order curves which are in a cycle of type (k, k). Then

$$q_1\mathbb{Z}[\zeta_k] = \prod_{1\leq m<k,(m,k)=1} (q_1, \zeta_k^m - q_2).$$

$$q_2\mathbb{Z}[\zeta_k] = \prod_{1\leq m<k,(m,k)=1} (q_2, \zeta_k^m - q_1).$$

If we focus on the case where $k \leq 36$, but $k \notin \{23, 29, 31\}$, the ideal class group becomes trivial and consequently, all ideals are principal. It could be very interesting to study this case since the applications require small embedding degrees (and 36 is a reasonable upper bound).

6.3.3 Cycles with even cyclotomic polynomial

In [7], the authors proved that $(5, 10)$, $(8, 8)$ and $(12, 12)$ cycles do not exist. The key observation was that for these values of k_1, k_2, $\Phi_{k_1}(x) = \Phi_{k_2}(-x)$ and $\deg \Phi_{k_1}(x) = 4$. Their proof sheds some light to other pairs for which $\Phi_{k_1}(x) = \Phi_{k_2}(-x)$. In particular (for our aim to study (k, k) cycles), k's such that $\Phi_k(x)$ is even polynomial are precisely those k's divisible by 4.

Lemma 6.12. [7, Part of Lemma 11.] Let k be a multiple of 4 and let $E_1/\mathbb{F}_{q_1}$, $E_2/\mathbb{F}_{q_2}$ be a 2-cycle of elliptic curves of type (k, k) such that $q_1 > q_2$ and let $c = q_1 - q_2$. Then $q_1 q_2 \mid \Phi_k(c)$.

Proposition 6.13. Let $E_1/\mathbb{F}_{q_1}, E_2/\mathbb{F}_{q_2}$ be a cycle of type $(4k, 4k)$ for some positive integer k. Then the values

$$m = \frac{q_1 + q_2}{2}, \quad n = \frac{q_1 - q_2}{2}, \quad d = \frac{\Phi_{4k}(|q_1 - q_2|)}{q_1 q_2},$$

satisfy the Diophantine equation

$$\Phi_{4k}(2n) + dn^2 = dm^2.$$

Proof. Let $E_1/\mathbb{F}_{q_1}, E_2/\mathbb{F}_{q_2}$ be a 2-cycle of elliptic curves of type $(4k, 4k)$ and let $c = q_1 - q_2$. Set $m = \frac{q_1+q_2}{2}$ and $n = \frac{q_1-q_2}{2}$. Clearly, $m, n \in \mathbb{Z}$ and Hasse bound says that $|n| < \sqrt{m}$. Now, by the previous lemma, write $\Phi_k(2n) = \Phi_k(c) = dq_1q_2 = d(m^2 - n^2)$. Then

$$\Phi_k(2n) + dn^2 = dm^2.$$

□

Example 6.14. Let us consider a special case where $4k = 16$. Then a $(16, 16)$-cycle can be found using an integral solution of the following Diophantine equation:

$$256n^8 + dn^2 + 1 = dm^2$$

More precisely, any $(16, 16)$-cycle gives rise to a solution (m, n, d). In particular, having all the integer solutions of the equation, we would find all $(16, 16)$-cycles or prove that there are no such. We point out that we have not found any positive integral solution to the mentioned equation (except the trivial one). We ran a computation showing that this equation does not have any solution for $1 \leq n \leq 10^5$ (see file `16_16_cycles.py` in the attachment). This means that $(16, 16)$-cycles do not exist for field sizes less than 10^{10}.

6.4 Cycle-friendly families

Our goal in this section is to characterize types of cycles, which can be achieved by families of elliptic curves.

This section aims to characterize the types of cycles, which can be achieved by 2-cycle-friendly families of elliptic curves.

Let $(q_k(x), r_k(x), t_k(x))$ be a family of elliptic curves and let s be the degree of $t_k(x)$. Since $r_k(x) \mid \Phi_k(t_k(x) - 1)$ and $q_k(x) \mid \Phi_{k'}(1 - t_k(x))$, Lemma 5.3 asserts that both $\varphi(k')$ and $\varphi(k)$ must divide $2s$. [24]

Proposition 6.15. Let k, k' be positive integers and $(q_k(x), r_k(x), t_k(x))$ be a family of prime-order elliptic curves with embedding degree k that is cycle-friendly for k' (and suppose also that both $q(x)$ and $r(x)$ represent primes and are integer-valued). Then both $\varphi(k)$ and $\varphi(k')$ divide $\deg q_k(x)$.

24. Recall that φ denotes the Euler totient function.

Proof. Since $\mathcal{F}$ is cycle-friendly for k', by Lemma 5.7 we have that $(r_k(x), q_k(x), 2 - t_k(x))$ is a family, which is cycle-friendly for k. By Lemma 5.8, $\varphi(k)$ divides $\deg r_k(x)$ and also $\varphi(k')$ divides $\deg q_k(x)$. Since $q_k(x)$ and $r_k(x)$ have the same degree, both $\varphi(k)$ and $\varphi(k')$ divide $\deg q_k(x)$. □

For example, there is no family with $\deg q_k(x) = 4$ that is cycle-friendly for embedding degree $p > 5$ for prime p.

6.5 Arbitrarily long cycles

So far we discussed the case of 2-cycles containing a curve from a family. Although, some of the discussion in the previous chapter sheds some light on arbitrary length cycles. Suppose we have an m-cycle of elliptic curves $E_1, E_2, \ldots, E_m$ with corresponding parameters $q_1, r_1, t_1, q_2, r_2, t_2, \ldots, q_m, r_m, t_m$. We know that $r_i = q_{i+1}$ for all $i < m$ and $r_m = q_1$.

First, we define a generalization of 2-cycle-friendliness presented in the previous section.

Definition 6.16. We say that a family of prime-order elliptic curves $(q_1(x), r_1(x), t_1(x))$ with embedding degree k_1 is m-cycle-friendly for embedding degrees $k_2, \ldots, k_m$, if there are polynomials $q_i(x), r_i(x)$, $t_i(x) = q_i(x) + 1 - r_i(x)$ for $2 \leq i \leq m$, such that

$$r_1(x) = q_2(x), \ldots, r_m(x) = q_1(x)$$

and $k_2, \ldots, k_m$ are minimal such that

$$r_2(x) \mid \Phi_{k_2}(t_2(x) - 1)$$

$$r_3(x) \mid \Phi_{k_3}(t_3(x) - 1)$$

$$\vdots$$

$$r_m(x) \mid \Phi_{k_m}(t_m(x) - 1).$$

Similarly, as in the case of 2-cycles, given a family that is m-cycle-friendly for some m-tuple of embedding degrees, we can construct cycles.

Proposition 6.17. Let $q_1(x), r_1(x), t_1(x)$ be a family with embedding degree k_1, that is cycle-friendly for embedding degrees $k_2, \ldots, k_m$. Then

(a) all but finitely many curves in the family $q_1(x), r_1(x), t_1(x)$ are in a cycle of type $(k_1, \ldots, k_m)$

(b) The degrees of the polynomials "match", that is

$$\deg q_1(x) = \ldots = \deg q_m(x).$$

Proof. If $r_i(x) \mid \Phi_{k_i}(t_i(x) - 1)$, then

$$r_i(m) \mid \Phi_{k_i}(t_i(m) - 1)$$

for any m, but we are not guaranteed that k_i is minimal such. But using the same discussion as in Theorem 5.5, there are only finitely many m's such that k_i is not minimal for that divisibility. Taking this over all i's, there are still at most finitely many m's for which some k_i is not minimal for the i-th divisibility. By Lemma 1.15 we get that all but finitely many curves in the family are in a $(k_1, \ldots, k_m)$-cycle.

The second observation is trivial from the fact that $r_i(x) = q_{i+1}(x)$. □

Corollary 6.18. The MNT3 family is m-cycle unfriendly for any tuple of embedding degrees.

Proof. Similarly as in Proposition 5.10, $\varphi(k) = 2$ (where φ is the Euler totient function), implying that the following embedding degree must be 3, 4 or 6. Therefore, all the embedding degrees must be 3, 4 or 6, but that is not possible due to Proposition 3.7. □

Summary

In this work, we presented elliptic curves, their families and cycles. We also briefly discussed their application in pairing-based cryptography and showed why the search for pairing-friendly cycles is essential.

In the previous works, it was known that for a high 2-adicity of Freeman or Barreto-Naehrig curves, one should take a highly 2-adic number x. We proved that this is the only way for Freeman curves, but we found that in the case of Barreto-Naehrig curves, a high 2-adicity can also be achieved by some odd numbers x. This could become very helpful with a combination of some other assumptions on the curve.

We also studied 2-cycles with the same embedding degree. We collected the known situation, proved some elementary cases, and in Section 6.3.2 we did a preliminary investigation of the prime factorization of ideals generated by field sizes of a cycle of type (k, k) for arbitrary k. We also propose a possible direction for improvements.

We summarized the main result of this work in Chapter 5. Given a lower bound on the field size, we gave a lower bound on the second embedding degree k in the cycles containing a curve from arbitrary family (of prime-order elliptic curves) $\mathcal{F}$. In Section 5.3 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 (given by Definition 1.16), implying that there are *no pairing-friendly 2-cycles of type* $(3, k)$ *for any* k. We also conjectured this statement in the case of Freeman and Barreto-Naehrig curves and justified our decision by two criteria: first, we used computational tools to prove our conjecture for $q \leq 2^{1200}$; and second, in Section 6.1 we sketched a possible proof for arbitrary families (since this case is "not that different" from the case of MNT3 cycles). However, we leave this problem unsolved.

In the last chapter, we add some interesting results and observations, which showed up during the research. We conclude the chapter with proof that cycle-friendly m-cycles do not contain curves with embedding degree 3.

Bibliography

1. BARRETO, Paulo S. L. M.; NAEHRIG, Michael. Pairing-Friendly Elliptic Curves of Prime Order. In: PRENEEL, Bart; TAVARES, Stafford (eds.). *Selected Areas in Cryptography*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 319–331. ISBN 978-3-540-33109-4.
2. BEN-SASSON, Eli; CHIESA, Alessandro; GENKIN, Daniel; TROMER, Eran; VIRZA, Madars. *SNARKs for C: Verifying Program Executions Succinctly and in Zero Knowledge* [Cryptology ePrint Archive, Report 2013/507]. 2013. `https://eprint.iacr.org/2013/507`.
3. BEN-SASSON, Eli; CHIESA, Alessandro; TROMER, Eran; VIRZA, Madars. *Scalable Zero Knowledge via Cycles of Elliptic Curves* [Cryptology ePrint Archive, Report 2014/595]. 2014 [visited on 2021-03-21]. Available from: `https://eprint.iacr.org/2014/595`.
4. BENGER, Naomi; SCOTT, Michael. *Constructing Tower Extensions for the implementation of Pairing-Based Cryptography* [Cryptology ePrint Archive, Report 2009/556]. 2009. `https://eprint.iacr.org/2009/556`.
5. BOWE, Sean; GRIGG, Jack; HOPWOOD, Daira. *Recursive Proof Composition without a Trusted Setup* [Cryptology ePrint Archive, Report 2019/1021]. 2019 [visited on 2021-03-26]. Available from: `https://eprint.iacr.org/2019/1021`.
6. BRÖKER, Reinier; STEVENHAGEN, Peter. Efficient CM-Constructions of Elliptic Curves over Finite Fields. *Mathematics of Computation*. 2007, vol. 76, no. 260, pp. 2161–2179. ISSN 00255718, ISSN 10886842. Available also from: `http://www.jstor.org/stable/40234483`.
7. CHIESA, Alessandro; CHUA, Lynn; WEIDNER, Matthew. *On cycles of pairing-friendly elliptic curves* [online]. 2018 [visited on 2021-03-06]. Available from arXiv: `1803.02067 [math.NT]`.

8. COMPANY, Electric Coin. *The Pasta Curves for Halo 2 and Beyond* [online] [visited on 2021-05-09]. Available from: https://electriccoin.co/blog/ecc-releases-code-for-halo-2/.

9. COX, D.A. *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*. Wiley, 2013. Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. ISBN 978-1-118-39018-4.

10. DUMMIT, David S.; FOOTE, Richard M. *Abstract algebra*. 3rd ed. Wiley, 2004.

11. FREEMAN, David. Constructing Pairing-Friendly Elliptic Curves with Embedding Degree 10. In: HESS, Florian; PAULI, Sebastian; POHST, Michael (eds.). *Algorithmic Number Theory*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 452–465. ISBN 978-3-540-36076-6.

12. FREEMAN, David; SCOTT, Michael; TESKE, Edlyn. A Taxonomy of Pairing-Friendly Elliptic Curves. *Journal of Cryptology* [online]. 2010, vol. 23, no. 2, pp. 224–280 [visited on 2021-03-06]. ISSN 1432-1378. Available from DOI: 10.1007/s00145-009-9048-z.

13. GABIZON, A. *Explaining SNARKs Part I* [online] [visited on 2021-05-04]. Available from: https://electriccoin.co/blog/snark-explain.

14. GALBRAITH, Steven D.; MCKEE, J.; VALENÇA, P. *Ordinary abelian varieties having small embedding degree* [Cryptology ePrint Archive, Report 2004/365]. 2004 [visited on 2021-03-06]. Available from: https://eprint.iacr.org/2004/365.

15. GALLANT, Robert P.; LAMBERT, Robert J.; VANSTONE, Scott A. Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms. In: KILIAN, Joe (ed.). *Advances in Cryptology — CRYPTO 2001*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 190–200. ISBN 978-3-540-44647-7.

16. HANSER, Christian. *New Trends in Elliptic Curve Cryptography* [online]. 2010 [visited on 2021-04-26]. Available from: https://diglib.tugraz.at/download.php?id=576a71d5e7117&location=browse. Master thesis. Institute for Applied Information Processing and Communications (IAIK), Graz University of Technology, Graz. Supervised by Dipl.-Ing. Dr.techn. Mario LAMBERGER.

17. HOFFSTEIN, Jeffrey; PIPHER, Jill; SILVERMAN, J.H. *An Introduction to Mathematical Cryptography*. 1st ed. Springer Publishing Company, Incorporated, 2008. ISBN 0387779930.

18. HOPWOOD, D. *The Pasta Curves for Halo 2 and Beyond* [online] [visited on 2021-05-09]. Available from: https://electriccoin.co/blog/the-pasta-curves-for-halo-2-and-beyond/.

19. KARABINA, Koray; TESKE, Edlyn. *On prime-order elliptic curves with embedding degrees $k = 3, 4$ and 6* [Cryptology ePrint Archive, Report 2007/425]. 2007 [visited on 2021-04-05]. Available from: https://eprint.iacr.org/2007/425.

20. KATE, Aniket; ZAVERUCHA, Gregory M.; GOLDBERG, Ian. Constant-Size Commitments to Polynomials and Their Applications. In: *Advances in Cryptology - ASIACRYPT 2010 - 16th International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2010, vol. 6477, pp. 177–194. Lecture Notes in Computer Science. Available from DOI: 10.1007/978-3-642-17373-8_11.

21. MIYAJI, Atsuko; NAKABAYASHI, Masaki; TAKANO, Shunzo. Characterization of Elliptic Curve Traces Under FR-Reduction. In: WON, Dongho (ed.). *Information Security and Cryptology — ICISC 2000*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 90–108. ISBN 978-3-540-45247-8.

22. SILVERMAN, Joseph H. *The Arithmetic of Elliptic Curves*. Dordrecht: Springer, 2009. Graduate texts in mathematics.

23. SILVERMAN, Joseph H.; STANGE, Katherine E. Amicable Pairs and Aliquot Cycles for Elliptic Curves. *Experimental Mathematics*. 2011, vol. 20, no. 3, pp. 329–357. ISSN 1944-950X. Available from DOI: 10.1080/10586458.2011.565253.

24. SILVERMAN, Joseph H.; TATE, John T. *Rational Points on Elliptic Curves*. 2nd. Springer Publishing Company, Incorporated, 2015. ISBN 331918587X.

25. TRAN, Anh Minh. *Párování na eliptických křivkách a jejich využití v kryptografii* [online]. 2019 [visited on 2021-04-29]. Available from: `https://is.muni.cz/th/w7yty/`. Bachelor's thesis. Masaryk University, Faculty of Science, Brno. Supervised by Vladimír SEDLÁČEK.

26. WASHINGTON, Lawrence C. *Elliptic Curves: Number Theory and Cryptography, Second Edition*. 2nd ed. Chapman & Hall/CRC, 2008. ISBN 9781420071467.