ELLIPTIC FERMAT NUMBERS AND ELLIPTIC DIVISIBILITY SEQUENCES

Seoyoung Kim
Department of Mathematics, Brown University, Providence, Rhode Island
seoyoung_kim@math.brown.edu

Alexandra Walsh
Department of Mathematics, Brown University, Providence, Rhode Island
alexandra_walsh@brown.edu

Received: 8/5/18, Revised: 12/5/19, Accepted: 4/10/20, Published: 5/8/20

Abstract

For a pair (E, P) of an elliptic curve $E/\mathbb{Q}$ and a nontorsion point $P \in E(\mathbb{Q})$, the sequence of elliptic Fermat numbers is defined by taking quotients of terms in the corresponding elliptic divisibility sequence $(D_n)_{n\in\mathbb{N}}$ with index powers of two, i.e. D_1, D_2/D_1, D_4/D_2, etc. Elliptic Fermat numbers share many properties with the classical Fermat numbers, $F_k = 2^{2^k} + 1$. In the present paper, we show that for magnified elliptic Fermat sequences, only finitely many terms are prime. We also define generalized elliptic Fermat numbers by taking quotients of terms in elliptic divisibility sequences that correspond to powers of any odd positive integer m, and show that many of the classical properties of Fermat numbers, including coprimality, order universality, and compositeness, still hold.

1. Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$ by a Weierstrass equation with rational coefficients

$$E : y^2 + a_1y + a_3xy = x^3 + a_2x^2 + a_4x + a_6. \tag{1}$$

We say (1) is minimal if the discriminant $|\Delta(E)|$ is minimal among all Weierstrass equations for E. Moreover, we say a minimal Weierstrass equation is reduced if $a_1, a_3 \in \{0, 1\}$ and $a_2 \in \{-1, 0, 1\}$. It is worth noting that for all elliptic curves over $\mathbb{Q}$, minimal models exist and a reduced minimal model is unique.

For a fixed nontorsion point $P \in E(\mathbb{Q})$, we can define the elliptic divisibility sequence as follows.

Definition 1. Let E be an elliptic curve defined over $\mathbb{Q}$ by a Weierstrass equation and choose a nontorsion point $P \in E(\mathbb{Q})$. The *elliptic divisibility sequence* (EDS)

associated with the pair (E, P) is the sequence $D = (D_n)_{n\in\mathbb{N}} : \mathbb{N} \to \mathbb{N}$ defined by taking the positive square root of the denominator of successive iterations of a fixed nontorsion point $P \in E(\mathbb{Q})$ as the lowest fraction, i.e.,

$$[n]P = \left(\frac{A_n}{D_n^2}, \frac{B_n}{D_n^3}\right), \tag{2}$$

where $\gcd(A_n, D_n) = \gcd(B_n, D_n) = 1$.

An EDS is minimal if the Weierstrass equation of $E/\mathbb{Q}$ is minimal and reduced. Much of our work revolves around elliptic Fermat numbers, analogues of the classical Fermat numbers ($F_n = 2^{2^n} + 1$, $n \geq 0$) defined by S. Binegar, R. Dominick, M. Kenney, J. Rouse, and A. Walsh in [1]. In the original version of the paper [2], they define elliptic Fermat numbers as follows:

Definition 2. Let E be an elliptic curve defined over $\mathbb{Q}$ by a Weierstrass equation and choose a nontorsion point $P \in E(\mathbb{Q})$. Let $D = (D_n)_{n\in\mathbb{N}}$ be an EDS associated with the pair (E, P). Define the sequence of *elliptic Fermat numbers* (EFN) $(F_k(E, P))_{k\in\mathbb{N}}$ as follows:

$$F_k(E,P) = \begin{cases} \frac{D_{2^k}}{D_{2^{k-1}}} & \text{if } k \geq 1, \\ D_1 & \text{if } k = 0. \end{cases}$$

Remark 1. The published version of the paper presents a slightly different definition of elliptic Fermat numbers than the one stated above. Namely, the authors define elliptic Fermat numbers as

$$\mathcal{F}_k(E, P) = B_k,$$

where B_k is the numerator of the lowest fraction of y-coordinate of $[k]P$, as in (2). The motivation for this change was to make elliptic Fermat numbers a closer analogue of classical Fermat numbers: Fermat's choice of sequence relied largely on the fact that $2^n + 1$ is composite when n is not a power of 2, and when put in the language of elliptic divisibility sequences, $2^n + 1$ corresponds to B_n. While this change provides stronger motivation for studying elliptic Fermat numbers, it does not largely alter the paper's results. We choose to use the original definition of EFN because it is in keeping with the notation of elliptic divisibility sequences and thus allows us to access a broad range of past results.

In [1, Theorem 7] (Also, please refer to [2, Theorem 9]), the authors show that the following seven conditions force $\mathcal{F}_k(E, P)$ to be composite for all $k \geq 1$. While they state that it is easy to check whether these conditions are satisfied, they are quite restrictive. Note that "egg" in Theorem 1 refers to the non-identity component of E, and that m_0 (used in condition (vi)) is the numerator of the lowest fraction of x-coordinate of P, as A_1 in (2).

Theorem 1. *For an elliptic curve $E : y^2 = x^3 + ax^2 + bx$, assume the following:*

(i) $E(\mathbb{Q}) = \langle P, T\rangle$*, where* P *has infinite order and* $T = (0, 0)$ *is a rational point of order* 2*;*

(ii) E *has an egg;*

(iii) T *is on the egg;*

(iv) T *is the only integral point on the egg;*

(v) P *is not integral;*

(vi) $\gcd(b, m_0) = 1$*;*

(vii) the equations $x^4 + ax^2y^2 + by^4 = \pm 1$ *have no integer solutions where* $y \notin \{0, \pm 1\}$*.*

Then $\mathcal{F}_k(E, P)$ *is composite for all* $k \geq 1$*.*

In the same vein, we prove the non-primality of a sequence of elliptic Fermat numbers defined by magnified elliptic divisibility sequences. First, we recall the definition of magnified elliptic divisibility sequences.

Definition 3. Let $E/\mathbb{Q}$ and $E'/\mathbb{Q}$ be two elliptic curves. We say a nontorsion point $P \in E(\mathbb{Q})$ is *magnified* if $P = \phi(P')$ for some (nonzero) isogeny $\phi : E' \to E$ over $\mathbb{Q}$ of degree $\deg(\phi) > 1$, and some nontorsion point $P' \in E'(\mathbb{Q})$. Moreover, an EDS $D = (D_n)_{n\in\mathbb{N}}$ is *magnified* if D is a minimal EDS associated with some magnified point on an elliptic curve over $\mathbb{Q}$. We call a sequence of elliptic Fermat numbers $(F_k(E, P))_{k\in\mathbb{N}}$ *magnified* if it is defined by using a magnified EDS.

We prove the following non-primality result about sequences of magnified elliptic Fermat numbers. The statement follows from Theorem 9 when $m = 2$.

Theorem 2. *Let $E/\mathbb{Q}$ be a minimal magnified elliptic curve with a fixed nontorsion point $P \in E(\mathbb{Q})$ having an isogeny $\phi : E' \to E$ of odd degree $\deg(\phi) > 1$ from a minimal elliptic curve $E'/\mathbb{Q}$ satisfying $\phi(P') = P$ for some nontorsion point $P' \in E'(\mathbb{Q})$. Then the terms $F_k(E, P)$ are composite for sufficiently large k.*

In this paper, we consider not only elliptic Fermat numbers, but also a generalization of these sequences. Generalized classical Fermat numbers have the form $a^{2^n} + b^{2^n}$ for some relatively prime integers a and b. It is natural to consider a similar generalization of elliptic Fermat numbers:

Definition 4. Let E be an elliptic curve defined over $\mathbb{Q}$ by a Weierstrass equation and choose a nontorsion point $P \in E(\mathbb{Q})$. Let $D = (D_n)_{n\in\mathbb{N}}$ be an EDS associated

with the pair (E, P), and let $m \geq 1$ be an integer. We define the sequence of *generalized elliptic Fermat numbers* $({F_k}^{(m)}(E,P))_{k\in\mathbb{N}}$ associated with the pair (E, P) as follows:

$${F_k}^{(m)}(E,P) = \begin{cases} \frac{D_{m^k}}{D_{m^{k-1}}} & \text{if } k \geq 1, \\ D_1 & \text{if } k = 0. \end{cases}$$

A sequence of generalized elliptic Fermat numbers associated with the pair (E, P) is minimal if the Weierstrass equation of $E/\mathbb{Q}$ is minimal and reduced. Note that Definition 2 is the special case where $m = 2$. In [1] and [2], they prove theorems regarding the common divisors of elliptic Fermat numbers and the so-called order universality of EFN, mirroring the coprimality and order universality of classical Fermat numbers. We show the following similar results about generalized EFN:

Theorem 3 (Coprimality). *Let $F = (F_k^{(m)}(E,P))_{k\in\mathbb{N}}$ be the sequence of minimal generalized elliptic Fermat numbers for a fixed elliptic curve E, a nontorsion point $P \in E(\mathbb{Q})$ and an odd integer $m \geq 1$. Then for all distinct $k, \ell \geq 0$,*

$$\gcd({F_k}^{(m)}(E,P), {F_\ell}^{(m)}(E,P)) \mid m.$$

Theorem 4 (Order Universality). *Let $F = (F_k^{(m)}(E,P))_{k\in\mathbb{N}}$ be the sequence of generalized elliptic Fermat numbers for a fixed elliptic curve E, a nontorsion point $P \in E(\mathbb{Q})$ and an odd integer $m \geq 1$. Then for all $N \in \mathbb{N}$ satisfying $\gcd(N, 6\Delta(E)) = 1$,*

$$P \text{ has order } m^k \text{ in } E(\mathbb{Z}/N\mathbb{Z})$$

if and only if

$$N \mid {F_0}^{(m)} \cdots {F_k}^{(m)} \text{ and } N \nmid {F_0}^{(m)} \cdots {F_{k-1}}^{(m)}.$$

Theorem 3 and Theorem 4 also hold for $m = 2$, please refer to [1, Theorem 2, Theorem 3] and [2, Theorem 3, Theorem 4] for more details. We also have a non-primality result for generalized elliptic Fermat numbers, which is motivated by various works on magnified elliptic sequences, such as [3].

Theorem 5. *Let $E/\mathbb{Q}$ be a minimal magnified elliptic curve with a fixed nontorsion point $P \in E(\mathbb{Q})$ having an isogeny $\phi : E' \to E$ of degree $\deg(\phi) > 1$ from a minimal elliptic curve $E'/\mathbb{Q}$ satisfying $\phi(P') = P$ for some nontorsion point $P' \in E'(\mathbb{Q})$. For m relatively prime to $\deg(\phi)$, $F_k^{(m)}(E,P)$ are composite for sufficiently large k.*

Note that in the main section of the paper we only prove results about generalized elliptic Fermat numbers, but the $m = 2$ case holds true for each of the more general theorems.

2. Properties of Generalized Elliptic Fermat Numbers

2.1. Coprimality

The authors of [1], motivated by the coprimality of the classical Fermat numbers, show that any prime dividing the greatest common divisor of two distinct elliptic Fermat numbers is a prime of bad reduction for the given elliptic curve. In this section, we prove a similar result for generalized elliptic Fermat numbers generated by odd m. We also generalize the order universality properties stated in [1, Theorem 3] and [1, Corollary 4].

Before proving any results, we present an example of a sequence of generalized elliptic Fermat numbers generated by $m = 3$.

Example 1. Let $E : y^2 = x^3 + x^2 - 4x$, $P = (-2, 2)$ and $m = 3$. The first four generalized elliptic Fermat numbers are listed below.

$P = (\frac{-2}{1^2}, \frac{2}{1^3})$	$F_0^{(3)}(E,P) = 1$
$3P = (\frac{-2}{3^2}, \frac{26}{3^3})$	$F_1^{(3)}(E,P) = \frac{3}{1} = 3$
$9P = (\frac{-213293858}{10593^2}, \frac{2478721052834}{10593^3})$	$F_2^{(3)}(E,P) = \frac{10593}{3} = 3531$
$27P = (\frac{-2387\ldots4098}{4777\ldots2659^2}, \frac{7135\ldots8638}{4777\ldots2659^3})$	$F_3^{(3)}(E,P) = \frac{4777\ldots2659}{10593} = 4509\ldots2163$ (33 digits)

We will now prove the following "coprimality" theorem, which states that the greatest common divisor of any two generalized elliptic Fermat numbers generated by an odd integer m must divide m.

Theorem 6 (Coprimality). *Let $F = (F_k^{(m)}(E,P))_{k\in\mathbb{N}}$ be the sequence of minimal generalized elliptic Fermat numbers for a fixed elliptic curve E, a nontorsion point $P \in E(\mathbb{Q})$ and an odd integer $m \geq 1$. Then for all distinct $k, \ell \geq 0$,*

$$\gcd(F_k{}^{(m)}(E,P), F_\ell{}^{(m)}(E,P)) \mid m.$$

The heart of the proof relies on the following lemma from [5]:

Lemma 1. *Let $D = (D_n)_{n\in\mathbb{N}}$ be a minimal EDS, let $n \geq 1$, and let p be a prime satisfying $p \mid D_n$.*

(a) For all $m \geq 1$ we have

$$\mathrm{ord}_p(D_{mn}) \geq \mathrm{ord}_p(mD_n).$$

(b) The inequality in (a) is strict,

$$\mathrm{ord}_p(D_{mn}) > \mathrm{ord}_p(mD_n),$$

if and only if $p = 2$, $2 \mid m$, $\mathrm{ord}_2(D_n) = 1$ *and* E *has ordinary or multiplicative reduction at* 2.

For our purposes, the conditions of (b) will never be met, since we are only working with odd m. Thus, we always have equality, i.e., if a prime p satisfies $p \mid D_n$, then

$$\mathrm{ord}_p(D_{mn}) = \mathrm{ord}_p(mD_n).$$

We can apply Lemma 1 to generalized elliptic Fermat numbers in the following way.

Proposition 1. *Let* $D = (D_n)_{n\in\mathbb{N}}$ *be a minimal EDS, and let* $m \geq 1$ *be an odd integer. If* $p \mid D_{m^{s-1}}$ *for some* $s \geq 1$*, then*

$$\mathrm{ord}_p({F_s}^{(m)}) = \mathrm{ord}_p(m).$$

Proof. Consider the case of Lemma 1 where $n = m^{s-1}$. Then if $p \mid D_{m^{s-1}}$ for some $s \geq 1$,

$$\mathrm{ord}_p(D_{m^s}) = \mathrm{ord}_p(mD_{m^{s-1}}).$$

It immediately follows that

$$\mathrm{ord}_p({F_s}^{(m)}) = \mathrm{ord}_p\left(\frac{D_{m^s}}{D_{m^{s-1}}}\right) = \mathrm{ord}_p(m).$$

□

We now use Proposition 1 to prove Theorem 6. For simplicity, we will let ${F_k}^{(m)}$ denote ${F_k}^{(m)}(E, P)$ whenever it appears in the rest of the paper.

Proof of Theorem 6. Let p be a prime, and suppose $p \mid D_{m^{s-1}}$ for some $s \geq 1$. Let $t = \min\{s \geq 1 : p \mid D_{m^{s-1}}\}$. Since $(D_n)_{n\in\mathbb{N}}$ is a divisibility sequence, it is given that $p \mid D_{m^{t-1}}$ implies $p \mid D_{m^{k-1}}$ for all $k \geq t$. Without loss of generality, we assume $k < \ell$ throughout the proof.

First, when $t \leq k < \ell$, Proposition 1 implies

$$\mathrm{ord}_p({F_k}^{(m)}) = \mathrm{ord}_p({F_\ell}^{(m)}) = \mathrm{ord}_p(m).$$

Thus, for each prime p that divides a term in $(D_n)_{n\in\mathbb{N}}$, and for all distinct $k, \ell \geq t$, we have

$$\mathrm{ord}_p(\gcd({F_k}^{(m)}, {F_\ell}^{(m)})) = \mathrm{ord}_p(m). \tag{3}$$

For all distinct k, ℓ with $k < t-1$, we have $p \nmid D_{m^k}$, which implies that p is not a factor of $\gcd({F_k}^{(m)}, {F_\ell}^{(m)})$. Hence, for all distinct k, ℓ with $k < t-1$, we have

$$\operatorname{ord}_p(\gcd({F_k}^{(m)}, {F_\ell}^{(m)})) = 0. \tag{4}$$

When $k = t-1$ and $\ell > k$, we have

$$p \nmid D_{m^{k-1}} \text{ and } p \mid D_{m^k}$$

and

$$p \mid D_{m^{\ell-1}} \text{ and } p \mid D_{m^\ell}.$$

Therefore, we have $\operatorname{ord}_p(F_k^{(m)}) \leq \operatorname{ord}_p(m)$ and $\operatorname{ord}_p(F_\ell^{(m)}) = \operatorname{ord}_p(m)$, and we get

$$\operatorname{ord}_p(\gcd({F_k}^{(m)}, {F_\ell}^{(m)})) \leq \operatorname{ord}_p(m). \tag{5}$$

From (3), (4), and (5), for any distinct k, ℓ, we have the desired result:

$$\gcd({F_k}^{(m)}, {F_\ell}^{(m)}) \mid m.$$

□

Remark 2. Theorem 6 actually implies a more specific result than the theorem states. For example, if $3 \mid {F_t}^{(15)}(E, P)$, then Theorem 6 only tells us that

$$\gcd({F_k}^{(15)}, {F_\ell}^{(15)}) \in \{1, 3, 5, 15\}$$

for all distinct $k, \ell \geq t$, but in actuality, we know that $\gcd({F_k}^{(15)}, {F_\ell}^{(15)}) \in \{3, 15\}$ because $3 \nmid 1$ and $3 \nmid 5$. In the case where m is prime, Theorem 6 gives an even more specific result, as stated in the corollary below.

Corollary 1. *Let $D = (D_n)_{n\in\mathbb{N}}$ be the minimal EDS for a fixed elliptic curve E and a nontorsion point $P \in E(\mathbb{Q})$, and let $F = (F_k^{(p^a)}(E, P))_{k\in\mathbb{N}}$ be the associated sequence of minimal generalized elliptic Fermat numbers defined by an odd prime power p^a. Then for all distinct $k, \ell \geq 0$,*

$$\gcd({F_k}^{(p^a)}(E, P), {F_\ell}^{(p^a)}(E, P)) \in \{1, p, p^2, \ldots, p^a\}.$$

In particular, for distinct $k, \ell \geq t$, we have

$$\gcd({F_k}^{(p^a)}(E, P), {F_\ell}^{(p^a)}(E, P)) \in \{1, p^a\},$$

where $t = \min\{s \geq 1 : p \mid D_{m^{s-1}}\}$.

Proof. The result follows from the proof of Theorem 6.

□

Example 2. We factor the generalized elliptic Fermat sequence from Example 1:

$$F_0^{(3)}(E,P) = 1$$

$$F_1^{(3)}(E,P) = \tfrac{3}{1} = 3$$

$$F_2^{(3)}(E,P) = \tfrac{10593}{3} = 3531 = 3 * 11 * 107$$

$$F_3^{(3)}(E,P) = \tfrac{4777\ldots2659}{10593} = 4509\ldots2163$$
$$= 3 * 3240769000879427 * 46385324158085723$$

We see that $\gcd({F_0}^{(3)}, {F_1}^{(3)}) = 1$, while $\gcd({F_k}^{(3)}, {F_\ell}^{(3)}) = 3$ for distinct $1 \leq k, \ell \leq 3$.

2.2. Order Universality

In addition to proving results about the greatest common divisor of elliptic Fermat numbers, the authors of [1] include a result connecting divisibility with order, which they call *order universality*. This property holds in full force for generalized elliptic Fermat numbers. In fact, the proofs are nearly the same as the proofs for the case where $m = 2$.

Theorem 7 (Order Universality). *Let $F = (F_k^{(m)})_{k\in\mathbb{N}}$ be the sequence of generalized elliptic Fermat numbers for a fixed elliptic curve E, a nontorsion point $P \in E(\mathbb{Q})$ and an odd integer $m \geq 1$. Then for all $N \in \mathbb{N}$ satisfying $\gcd(N, 6\Delta(E)) = 1$,*

$$P \text{ has order } m^k \text{ in } E(\mathbb{Z}/N\mathbb{Z})$$

if and only if

$$N \mid {F_0}^{(m)} \cdots {F_k}^{(m)} \text{ and } N \nmid {F_0}^{(m)} \cdots {F_{k-1}}^{(m)}.$$

Proof. The proof follows the exact same steps as the proof of Theorem 3 in [1]. Namely, we define a homomorphism $\phi : E(\mathbb{Q}) \to E(\mathbb{Z}/N\mathbb{Z})$ that maps $P \mapsto P \pmod N$, then use the fact that $\phi(p^k P) = p^k \phi(P)$ to demonstrate that P has order m^k in $E(\mathbb{Z}/N\mathbb{Z})$ exactly when $N \mid {F_0}^{(m)} \cdots {F_k}^{(m)}$ and $N \nmid {F_0}^{(m)} \cdots {F_{k-1}}^{(m)}$. □

Corollary 2. *Let $F = (F_k^{(m)})_{k\in\mathbb{N}}$ be the sequence of minimal generalized elliptic Fermat numbers for a fixed elliptic curve E, a nontorsion point $P \in E(\mathbb{Q})$ and an odd integer $m \geq 1$. Let p be an odd prime such that $p \nmid 6m\Delta(E)$. Then*

$$P \text{ has order } m^k \text{ in } E(\mathbb{F}_p) \quad \text{if and only if} \quad p \mid {F_k}^{(m)}.$$

Proof. The proof is similar to that of Corollary 4 in [1]. However, whereas the proof in [1] relies on the fact that $\gcd({F_k}^{(2)}, {F_\ell}^{(2)}) \in \{1, 2\}$, here we require that $p \nmid m$ in order to make use of Theorem 3, which tells us that $\gcd({F_k}^{(m)}, {F_\ell}^{(m)}) \mid m$. The adapted proof proceeds as follows: If $p \mid {F_0}^{(m)} \cdots {F_k}^{(m)}$ and $p \nmid {F_0}^{(m)} \cdots {F_{k-1}}^{(m)}$, then $p \mid {F_k}^{(m)}$. Conversely, if $p \mid {F_k}^{(m)}$, then $p \mid {F_0}^{(m)} \cdots {F_k}^{(m)}$. Theorem 3 gives us $p \nmid {F_i}^{(m)}$ for all $i \neq k$, implying $p \nmid {F_0}^{(m)} \cdots {F_{k-1}}^{(m)}$. Thus we have shown that $p \mid {F_k}^{(m)}$ if and only if $p \mid {F_0}^{(m)} \cdots {F_k}^{(m)}$ and $p \nmid {F_0}^{(m)} \cdots {F_{k-1}}^{(m)}$, and the desired result follows from Theorem 7. □

Example 3. Using the curve E, point P and integer m from Example 1, observe that the order of $P \in E(\mathbb{F}_{593}) = 3^2$, and indeed, $593 \mid {F_2}^{(3)} = 3 * 593 = 1779$.

3. Compositeness of Magnified Generalized Elliptic Fermat Numbers

3.1. Primality Conjecture for Generalized Elliptic Fermat Numbers

Throughout this section, we assume E to be an elliptic curve over $\mathbb{Q}$ and $P \in E(\mathbb{Q})$ to be a nontorsion point. Everest, Miller, and Stephens [3] proved the following conjecture for *magnified* elliptic divisibility sequences.

Conjecture 1 (Primality conjecture). Let $D = (D_n)_{n\in\mathbb{N}}$ be an elliptic divisibility sequence associated with the pair (E, P). Then $D = (D_n)_{n\in\mathbb{N}}$ contains only finitely many prime terms.

Note that for the Fibonacci sequence, it is conjectured that primes occur infinitely many times. In this section, we will prove the following conjecture for magnified generalized elliptic Fermat numbers.

Conjecture 2 (Primality conjecture for generalized elliptic Fermat numbers). Let $F = (F_k^{(m)}(E, P))_{k\in\mathbb{N}}$ be the sequence of generalized elliptic Fermat numbers for an elliptic curve E and a fixed nontorsion point $P \in E(\mathbb{Q})$. Then $F = (F_k^{(m)}(E, P))_{k\in\mathbb{N}}$ contains only finitely many prime terms.

Using Corollary 2, we can prove the following result.

Lemma 2. *Let $E/\mathbb{Q}$ be a minimal magnified elliptic curve with a fixed nontorsion point $P \in E(\mathbb{Q})$ having an isogeny $\phi : E' \to E$ of degree $d = \deg(\phi) > 1$ from a minimal elliptic curve $E'/\mathbb{Q}$ satisfying $\phi(P') = P$ for some nontorsion point $P' \in E'(\mathbb{Q})$. For sufficiently large k and m with $\gcd(m, d) = 1$, we have*

$$\gcd(F_k^{(m)}(E', P'), F_k^{(m)}(E, P)) \neq 1. \tag{6}$$

Proof. Let p be a fixed prime which divides $F_k^{(m)}(E', P')$. Let S be the set of primes for which E and E' have bad reduction, where ϕ cannot be reduced to give

an isogeny on elliptic curves E and E' modulo p. Note that S is a finite set. Thus, we consider sufficiently large k so that $p \notin S$, which is possible from Theorem 3. If $p \mid m$, we have (6) for large enough k by Proposition 1. Otherwise, from Corollary 2, it is sufficient to prove that the isogeny ϕ reduced modulo p (which is again an isogeny) preserves the order m^k of P',

$$\phi : E'(\mathbb{F}_p) \to E(\mathbb{F}_p).$$

We consider the dual isogeny $\hat{\phi}$ of ϕ. We know

$$\hat{\phi} \circ \phi = [d],$$

where $[d]$ is the multiplication-by-d map on E'. Then the map

$$[d] : E'(\mathbb{F}_p) \xrightarrow{\phi} E(\mathbb{F}_p) \xrightarrow{\hat{\phi}} E'(\mathbb{F}_p)$$

preserves the order m^k of P' and so does ϕ. □

Example 4. We can see the divisibility of corresponding elliptic Fermat numbers using the following magnified elliptic divisibility sequence, which has a degree 3 isogeny ϕ that maps

$$E_1' : y^2 = x^3 - 9x + 9, \quad \text{with } P' = [1, 1]$$

to

$$E_1 : y^2 = x^3 - 189x - 999, \quad \text{with } P = [-8, 1].$$

Then we get the following factorizations, and we can check the divisibility of corresponding elliptic Fermat numbers.

$F_1(E_1', P') = 1$	$F_1(E_1, P) = 2$
$F_2(E_1', P') = 17$	$F_2(E_1, P) = 2 * 17 * 19$
$F_3(E_1', P') = 53 * 127$	$F_3(E_1, P) = 2 * 53 * 127 * 10799 * 14867$
$F_4(E_1', P') = 89 * 179 * 307 * 5813 * 838133$	$F_4(E_1, P) = 2 * 89 * 179 * 307 * 757 * 5813 * 67211 * 838133 * 265666679 * 3205176128020873$
$\vdots$	$\vdots$

Similarly, for a degree 7 isogeny which maps

$$E_2' : y^2 + xy = x^3 - x^2 + x + 1, \quad \text{with } Q' = [0, 1]$$

to

$$E_2 : y^2 + xy = x^3 - x^2 - 389x - 2859, \quad \text{with } Q = [26, 51],$$

we have

$F_1(E_2', Q') = 1$	$F_1(E_2, Q) = 1$
$F_2(E_2', Q') = 3$	$F_2(E_2, Q) = 3 * 701$
$F_3(E_2', Q') = 11$	$F_3(E_2, Q) = 11 * 233 * 2887 * 273001$
$F_4(E_2', Q') = 1523 * 15443$	$F_4(E_2, Q) = 103 * 131 * 311 * 467 * 1523 * 11831$ $* 15443 * 12539851$ $* 7015932452763098743789$
$\vdots$	$\vdots$

Example 5. We can see the divisibility of corresponding generalized elliptic Fermat numbers using the following magnified elliptic divisibility sequence, which has a degree 2 isogeny ϕ that maps

$$E' : y^2 = x^3 + x^2 - 4x, \quad \text{with } P' = [-2, 2]$$

to

$$E : y^2 = x^3 + x^2 + 16x + 16 \quad \text{with } P = [0, 4].$$

Then we get the following list of $F_k^{(3)}(E', P')$ and $F_k^{(3)}(E, P)$.

$F_1^{(3)}(E', P') = 3$	$F_1^{(3)}(E, P) = 3$
$F_2^{(3)}(E', P') = 3 * 11 * 107$	$F_2^{(3)}(E, P) = 3 * 11 * 23 * 107 * 449$
$F_3^{(3)}(E', P') = 3 * 3240769000879427$ $* 46385324158085723$	$F_3^{(3)}(E, P) = 3 * 114078700999$ $*3240769000879427$ $*46385324158085723$ $*927508107491526089159$
$\vdots$	$\vdots$

3.2. Compositeness of Magnified Generalized Elliptic Fermat Numbers

Following the idea in [3], we consider the growth of generalized elliptic Fermat numbers and the compositeness of all but finitely many magnified generalized elliptic Fermat numbers.

Definition 5. Let $E/\mathbb{Q}$ be an elliptic curve with a point $P \in E(\mathbb{Q})$, denoted as $P = \left(\frac{A}{D^2}, \frac{B}{D^3}\right)$. We define the *height* of a point $h(P)$ by using its x-coordinate:

$$h(P) = \log(\max(|A|, D^2)).$$

Moreover, we define the *canonical height* of a point $\hat{h}(P)$ by

$$\hat{h}(P) = \lim_{k \to \infty} \frac{h(2^k P)}{4^k}.$$

Remark 3. Note that when we have $[l]P = \left(\frac{A_l}{D_l^2}, \frac{B_l}{D_l^3}\right)$ with $\gcd(A_l, D_l) = 1$, the strong version of Siegel's theorem [4, VIII] implies

$$\lim_{l\to\infty} \frac{\log(D_l^2)}{l^2} = \lim_{l\to\infty} \frac{\log|A_l|}{l^2} = \hat{h}(P).$$

For instance, if we choose $l = 3^k$ for some k, we can also represent

$$\hat{h}(P) = \lim_{k\to\infty} \frac{\log(D_{3^k}^2)}{9^k} = \lim_{k\to\infty} \frac{\log|A_{3^k}|}{9^k}.$$

From Remark 3, we can also describe the growth of generalized elliptic Fermat numbers using the canonical height of P.

Theorem 8. *Let $E/\mathbb{Q}$ be an elliptic curve with a fixed point $P \in E(\mathbb{Q})$. Denote by $\hat{h}(P)$ the canonical height of P. For any m, we get*

$$\lim_{k\to\infty} \frac{\log(F_k^{(m)}(E,P))}{m^{2k}} = \left(\frac{1}{2} - \frac{1}{2m^2}\right) \cdot \hat{h}(P).$$

Proof. We have

$$\begin{aligned}
\lim_{k\to\infty} \frac{\log(F_k^{(m)}(E,P))}{m^{2k}} &= \lim_{k\to\infty} \frac{\log\left(\frac{D_{m^k}}{D_{m^{k-1}}}\right)}{m^{2k}} \\
&= \lim_{k\to\infty} \frac{\log(D_{m^k})}{m^{2k}} - \lim_{k\to\infty} \frac{\log(D_{m^{k-1}})}{m^{2k}} \\
&= \lim_{k\to\infty} \frac{1}{2} \cdot \frac{\log(D_{m^k}^2)}{m^{2k}} - \lim_{k\to\infty} \frac{1}{2m^2} \cdot \frac{\log(D_{m^{k-1}}^2)}{m^{2(k-1)}} \\
&= \left(\frac{1}{2} - \frac{1}{2m^2}\right) \cdot \hat{h}(P).
\end{aligned}$$

□

Using Lemma 2 and Theorem 8, we can prove the primality conjecture for magnified generalized elliptic Fermat numbers.

Theorem 9. *Let $E/\mathbb{Q}$ be a minimal magnified elliptic curve with a fixed nontorsion point $P \in E(\mathbb{Q})$ having an isogeny $\phi : E' \to E$ of degree $\deg(\phi) > 1$ from a minimal elliptic curve $E'/\mathbb{Q}$ satisfying $\phi(P') = P$ for some nontorsion point $P' \in E'(\mathbb{Q})$. For m relatively prime to $\deg(\phi)$, $F_k^{(m)}(E,P)$ are composite for sufficiently large k.*

Proof. Using Siegel's Theorem, we know

$$\hat{h}(P) = d\hat{h}(P'),$$

where d is the degree of the given isogeny ϕ. Therefore, for sufficiently large k, there is a prime divisor which is a proper divisor of $F_k^{(m)}(E,P)$ by Lemma 2 and Theorem 8. □

Acknowledgements. We would like to thank the 2017 Wake Forest University REU research group, whose work in defining and proving properties of elliptic Fermat numbers inspired our investigation of generalized elliptic Fermat numbers. We would especially like to thank Professor Jeremy Rouse, who led the Wake Forest research project, for providing feedback during the writing of this paper. We are also grateful to Professor Joseph Silverman and Yuwei Zhu for their helpful advising. Finally, we would like to thank the Directed Reading Program at Brown University, which enabled us to collaborate, and the anonymous referee for helpful comments.

References

[1] S. Binegar, R. Dominick, M. Kenney, J. Rouse, and A. Walsh, An elliptic curve analogue to the Fermat numbers, *Involve* **12(3)** (2019), 427-449.

[2] S. Binegar, R. Dominick, M. Kenney, J. Rouse, and A. Walsh, An elliptic curve analogue to the Fermat numbers, `https://arxiv.org/abs/1708.03804`, preprint (2017).

[3] G. Everest, V. Miller, and N. Stephens, Primes generated by elliptic curves, *Proc. Amer. Math. Soc.* **132(4)** (2004), 955-963.

[4] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.

[5] J. H. Silverman and K. E. Stange, Terms in elliptic divisibility sequences divisible by their indices, *Acta Arith.* **146(4)** (2011), 355-378.