involve

a journal of mathematics

An elliptic curve analogue to the Fermat numbers

Skye Binegar, Randy Dominick,
Meagan Kenney, Jeremy Rouse and Alex Walsh

msp

2019 vol. 12, no. 3

INVOLVE 12:3 (2019)
dx.doi.org/10.2140/involve.2019.12.427

An elliptic curve analogue to the Fermat numbers

Skye Binegar, Randy Dominick,
Meagan Kenney, Jeremy Rouse and Alex Walsh

(Communicated by Bjorn Poonen)

The Fermat numbers have many notable properties, including order universality, coprimality, and definition by a recurrence relation. We use rational points of infinite order on elliptic curves to generate sequences that are analogous to the Fermat numbers. We demonstrate that these sequences have many of the same properties as the Fermat numbers, and we discuss results about the prime factors of sequences generated by specific curves and points.

1. Introduction

In August 1640, Fermat wrote a letter to Frénicle [Fermat 1894, p. 205] recounting his discovery that if n is not a power of 2, then 2^n+1 is composite. Fermat also stated that if n is a power of 2, then 2^n+1 is prime. As examples, he listed the first seven numbers in this sequence, $F_n = 2^{2^n}+1,\ n \geq 0$, now called the sequence of Fermat numbers.

In 1732, Euler discovered that Fermat's observation was incorrect, and that 641 divides $F_5 = 4294967297$. Indeed, it is now known that F_n is composite for $5 \leq n \leq 32$. Very little is known about whether any F_n are prime; heuristics suggest that only finitely many of them are prime. However, mathematicians have been unable to prove that there are infinitely many composite Fermat numbers.

The primality of the Fermat numbers is connected with the classical problem of constructing a regular polygon with n sides using only an unmarked straightedge and a compass. In 1801, Gauss proved that if a positive integer n is a power of 2 multiplied by a product of distinct Fermat primes, then a regular n-gon is constructible with a ruler and compass. The converse of this result was proven by Wantzel in 1837. (For a modern proof, see [Dummit and Foote 2004, p. 602].)

Elliptic curves are central objects in modern number theory and have led to novel methods of factoring [Lenstra 1987b], proofs that numbers are prime [Atkin

MSC2010: primary 11G05; secondary 11B37, 11G15, 11Y11.
Keywords: elliptic curves, Fermat numbers, duplication formula.
All authors were supported by NSF grant DMS-1461189.

and Morain 1993], and cryptography [Koblitz 1987; Miller 1986]. They have also played a role in a number of important theoretical developments, the most spectacular of which is the "modular method" that led to the solution of Fermat's last theorem [Wiles 1995]. Other such developments include the determination of all integer solutions to $x^2 + y^3 = z^7$ with $\gcd(x, y, z) = 1$ [Poonen et al. 2007] and the determination of all perfect powers in the Fibonacci sequence [Bugeaud et al. 2006]. The present paper relies on both elliptic curves and the sequence of Fermat numbers. We work with elliptic curves in the form $E : y^2 = x^3 + ax^2 + bx + c$. We begin with our central definition:

Definition 1. For an elliptic curve E and a point $P \in E(\mathbb{Q})$ of infinite order, let $2^k P = (m_k/e_k^2, n_k/e_k^3)$ denote P added to itself 2^k times under the group law on $E(\mathbb{Q})$. Here $m_k, n_k, e_k \in \mathbb{Z}$ with $e_k \geq 1$ and $\gcd(m_k, e_k) = \gcd(n_k, e_k) = 1$. We define the sequence of *elliptic Fermat numbers* $\{F_k(E, P)\}$ by $F_k(E, P) = n_k$.

Fermat's observation that if n is not a power of 2, then $2^n + 1$ is not prime can be explained as follows. If b is an odd divisor of n, and q is a prime divisor of $2^{n/b}+1$, then $2^{n/b} \equiv -1 \pmod{q}$ (so $2^{n/b}$ has order 2 in $\mathbb{F}_p^\times = \mathbb{G}_m(\mathbb{F}_p)$). Then $2^n \equiv (-1)^b \equiv -1 \pmod{q}$ and so $q \mid 2^n + 1$. Since $q \leq 2^{n/b} + 1 < 2^n + 1$, the number $2^n + 1$ cannot be prime.

We are essentially replacing $\mathbb{G}_m$ with an elliptic curve E. If $P \in E(\mathbb{Q})$ is a point on E, p is a prime of good reduction for E, and $nP = (a_n/b_n^2, c_n/b_n^3)$, then $nP \in E(\mathbb{F}_p)$ has order 2 if and only if the y-coordinate of nP reduces to 0 mod p, that is, $p \mid c_n$. As above, if b is an odd divisor of n and there is a prime q of good reduction for E so that $q \mid |c_{n/b}|$, then $q \mid c_n$. It follows that c_n cannot be prime unless $|c_{n/b}| = |c_n|$, or all prime factors of $c_{n/b}$ are in S, the set of primes of bad reduction for E.

The growth rate of the numbers c_n implies that $|c_{n/b}| = |c_n|$ for only finitely many n. The group law on E implies that if all prime factors of $c_{n/b}$ are in S, then $2(n/b)P$ is an S-integral point, of which there are only finitely many on E (and in some cases, none).

It follows that possibilities for c_n to be prime when n has an odd divisor are very constrained. For this reason, we choose to focus on the case where n does not have any odd divisors, namely when n is a power of 2. This leads directly to our definition of elliptic Fermat numbers above.

Our goal is to show that the sequence $\{F_k(E, P)\}$ strongly resembles the classic Fermat sequence. We do so by adapting properties of the classic Fermat numbers and proving that they hold for the elliptic Fermat numbers. It is well known, for example, that any two distinct classic Fermat numbers are relatively prime, as Goldbach proved in a 1730 letter to Euler. The elliptic Fermat numbers have a similar property:

Theorem 2. *For all $k \neq \ell$, if p is a prime that divides* $\gcd(F_k(E, P), F_\ell(E, P))$, *then p is a prime of bad reduction for $E : y^2 = x^3 + ax^2 + bx + c$.*

The classic Fermat numbers also have the useful property that for any nonnegative integer N, 2 has order 2^{k+1} in $(\mathbb{Z}/N\mathbb{Z})^\times$ if and only if $N \mid F_0 \cdots F_k$ and $N \nmid F_0 \cdots F_{k-1}$. This property, which we call *order universality*, provides a powerful connection between order and divisibility. A close parallel applies to the elliptic Fermat numbers:

Theorem 3. *Let $\Delta(E)$ be the discriminant of E and suppose that N is a positive integer with* $\gcd(N, 6\Delta(E)) = 1$. *Then P has order 2^{k+1} in $E(\mathbb{Z}/N\mathbb{Z})$ if and only if $N \mid F_0(E, P) \cdots F_k(E, P)$ and $N \nmid F_0(E, P) \cdots F_{k-1}(E, P)$.*

In the case where $N = p$ for some odd prime p, we can make this statement stronger. For the classic Fermat numbers, we know that 2 has order 2^{k+1} in $\mathbb{F}_p^\times$ if and only if $p \mid F_k$. The elliptic Fermat numbers yield the following result:

Corollary 4. *For any odd prime $p \nmid 6\Delta(E)$, P has order 2^{k+1} in $E(\mathbb{F}_p)$ if and only if $p \mid F_k(E, P)$.*

This corollary plays a role in several important results in the paper.

Additionally, and quite interestingly, the classic Fermat numbers can be defined by several different recurrence relations. In Section 4, we present the following analogous result:

Theorem 5. *Let $E : y^2 = x^3 + ax^2 + bx + c$ be an elliptic curve, and let $P \in E(\mathbb{Q})$ be a point of infinite order. There is a sequence of integers $\{\tau_k\}$ so that*

$$m_k(E, P) = \frac{1}{\tau_k^2}(m_{k-1}^4 - 2bm_{k-1}^2 e_{k-1}^4 - 8cm_{k-1}e_{k-1}^6 + b^2 e_{k-1}^8 - 4ace_{k-1}^8), \tag{1}$$

$$\begin{aligned} F_k(E, P) = \frac{1}{\tau_k^3}\big(&-2am_{k-1}m_k e_{k-1}^2 \tau_k^2 - 4bm_{k-1}e_{k-1}^4 F_{k-1}^2 - bm_k e_{k-1}^4 \tau_k^2 \\ &- 8ce_{k-1}^6 F_{k-1}^2 + 4m_{k-1}^3 F_{k-1}^2 - 3m_{k-1}^2 m_k \tau_k^2\big), \end{aligned} \tag{2}$$

$$e_k(E, P) = \frac{1}{\tau_k}(2F_{k-1}e_{k-1}). \tag{3}$$

Unlike the various classic Fermat recurrence relations, which only depend on previous terms, the elliptic Fermat recurrence relation we have discovered relies on several other sequences of integers, namely m_k, e_k, and τ_k.

This equation follows naturally from the definition of $F_k(E, P)$ and the duplication formula, which we will see in Section 2. In order to have a true recurrence relation, however, we need a way to explicitly calculate $|\tau_k|$. Luckily, we know the following fact:

Theorem 6. *The $|\tau_k|$ are eventually periodic, and there is an algorithm to compute $|\tau_k|$ for all k.*

In Section 5, we address one of the most famous aspects of the classic Fermat numbers: the question of their primality. Whereas the primality of the Fermat numbers remains an open question, the following result gives conditions under which the elliptic Fermat numbers are always composite. In this result, "the egg" refers to the nonidentity component of the real points of the elliptic curve:

Theorem 7. *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 equation $x^4+ax^2y^2+by^4 = \pm 1$ has no integer solutions where $y \notin \{0, \pm 1\}$.*

Then $F_k(E, P)$ is composite for all $k \geq 1$.

Remark. There are many theorems in the literature about the compositeness of coordinates of rational points on elliptic curves that are in the image of an isogeny; see for example the main theorem of [Everest et al. 2004], and Theorem 1.4 of [Everest et al. 2008]. One feature of the result above in contrast with others is that we give an explicit set of conditions which guarantees that F_k is composite for all k.

Remark. We wish to note that given a rank-1 curve E and a point $P \in E(\mathbb{Q})$, there is an algorithm that can check whether the conditions in the theorem are satisfied. The condition that $x^4 + ax^2y^2 + by^4 = 1$ has no integer solutions where $y \notin \{0, \pm 1\}$ can also be checked with finitely many calculations, as this is a Thue equation. Such an equation has finitely many solutions [Thue 1909], and the solutions can be found effectively [Tzanakis and de Weger 1989].

There are choices of E for which all seven of the above conditions are satisfied. For example, we can take $E : y^2 = x^3 - 199x^2 - x$. Note that $\Delta(E)$ is positive and thus E has an egg [Silverman 1994, p. 420]. The only integral point on the curve is $T = (0, 0)$, which must be on the egg because 0 is in-between the x-coordinates of the other two roots of the polynomial. Also, $2T = (0 : 1 : 0)$ and thus T is a rational point of order 2 on E. The generating point of the curve is $P = \left(\frac{2809}{9}, \frac{89623}{27}\right)$, and $\gcd(-1, 2809) = 1$. Finally, Magma [Bosma et al. 1997] can be used to solve Thue equations in order to conclude that there are no integer solutions to $x^4 - 199x^2y^2 - y^4 = \pm 1$ where $y \notin \{0, \pm 1\}$. Thus this example satisfies the conditions for the theorem, and so F_k is composite for all k.

Section 6 focuses on the growth rate of the elliptic Fermat numbers. Much like the classic Fermat numbers, the elliptic Fermat numbers grow at a doubly exponential rate:

Theorem 8. *Let F_k be the k-th elliptic Fermat number in the sequence generated by the elliptic curve E and the point $P = (m_0/e_0^2, n_0/e_0^3)$. If $\hat{h}(P)$ denotes the canonical height of P, then*

$$\lim_{k\to\infty} \frac{\log(F_k)}{4^k} = \tfrac{3}{2}\hat{h}(P).$$

The proof is straightforward and is based on the properties of the $\{\tau_k\}$ sequence and the theory of height functions.

Finally, in Section 7, we examine the curve $E : y^2 = x^3 - 2x$ and the elliptic Fermat sequence generated by the point $P = (2, 2)$. It is a theorem of Lucas that a prime divisor of the Fermat sequence is congruent to 1 mod 2^{n+2}. Upon examination of the factorization of the numbers in the sequence $\{F_n(E, P)\}$, we arrive at a pleasing congruence analogue:

Theorem 9. *Let $E : y^2 = x^3 - 2x$ and consider the point $P = (2, 2)$ and the elliptic Fermat sequence $(F_n(E, P))$. For any prime p such that $p \mid F_n(E, P)$ for some n, we have*

$$p \equiv \begin{cases} 1 \pmod{2^{n+1}} & \text{if } p \equiv 1 \pmod 4, \\ -1 \pmod{2^{n+1}} & \text{if } p \equiv -1 \pmod 4. \end{cases}$$

In addition to this congruence result, we have a partial converse that tells us about the presence of Fermat and Mersenne primes in $(F_n(E, P))$:

Theorem 10. *For $E : y^2 = x^3 - 2x$, consider the point $P = (2, 2)$. Let $F_k = 2^{2^k} + 1$ be a Fermat prime and $F_k \neq 5, 17$. Then F_k divides $F_n(E, P)$ for some $n \leq 2^{k-1} - 2$.*

Theorem 11. *For $E : y^2 = x^3 - 2x$, consider the point $P = (2, 2)$. Let $q = 2^p - 1 \geq 31$ be a Mersenne prime. Then q divides $F_n(E, P)$ for some $n \leq p - 4 \in \mathbb{N}$.*

2. Background

We begin with some general background on elliptic curves. For the purposes of this paper, an elliptic curve is a nonsingular cubic curve defined over $\mathbb{Q}$ that has the form $y^2 = x^3 + ax^2 + bx + c$ for some $a, b, c \in \mathbb{Z}$. When we say E is nonsingular, we mean that there are no singular points on the curve. We will often think of E as living in $\mathbb{P}^2$ and represent it with the homogeneous equation $y^2z = x^3 + ax^2z + bxz^2 + cz^3$. A *singular point* is a point $P = (x : y : z)$ at which there is not a well-defined tangent line. These points occur when the following equations are equal to 0:

$$F(x, y, z) = y^2z - x^3 - ax^2z - bx^2z - cz^3,$$
$$\frac{\partial F}{\partial x} = -3x^2 - 2azx - bz^2, \quad \frac{\partial F}{\partial y} = 2yz, \quad \frac{\partial F}{\partial z} = y^2 - ax^2 - 2bxz - 3cz^2. \tag{4}$$

We write $E(\mathbb{Q})$ to denote the set of rational points on E along with the point at infinity, $(0:1:0)$. Using the following binary operation, we can give $E(\mathbb{Q})$ a group structure: for $P, Q \in E(\mathbb{Q})$, draw a line through P and Q and let $R = (x, y)$ be the third intersection point of the line with the curve. Then $P + Q = (x, -y)$. This operation gives an abelian group structure on $E(\mathbb{Q})$ with $(0:1:0)$ as the identity.

Any $P \in E(\mathbb{Q})$ can be expressed in projective space as $P = (m/e^2 : n/e^3 : 1) = (me : n : e^3)$ for some $m, n, e \in \mathbb{Z}$ with $\gcd(m, e) = \gcd(n, e) = 1$. From this, there is a well-defined map from $E(\mathbb{Q}) \to E(\mathbb{F}_p)$ that takes $(me : n : e^3)$ to $(me \bmod p : ne \bmod p : e^3 \bmod p)$; this map is a homomorphism if $E/\mathbb{F}_p$ is nonsingular. We have $P \equiv (0:1:0) \pmod{p}$ if and only if $p \mid e$.

Let $\mathbb{Q}_p$ be the field of p-adic numbers. The following sets are subgroups of $E(\mathbb{Q}_p)$:

$$\begin{aligned} E_0(\mathbb{Q}_p) &= \{P \in E(\mathbb{Q}_p) \mid P \text{ reduces to a nonsingular point}\}, \\ E_1(\mathbb{Q}_p) &= \{P \in E(\mathbb{Q}_p) \mid P \text{ reduces to } (0:1:0) \bmod p\}. \end{aligned} \tag{5}$$

We have $E_1(\mathbb{Q}_p) \subseteq E_0(\mathbb{Q}_p) \subseteq E(\mathbb{Q}_p)$, and the index $[E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)]$ is finite and is called the *Tamagawa number* of E at p.

The *discriminant* of an elliptic curve E is defined as

$$\Delta(E) = 64a^3c + 16a^2b^2 + 288abc - 64b^3 - 432c^2.$$

The set $E(\mathbb{R})$ can have one or two components depending on whether or not $\Delta(E) < 0$ or $\Delta(E) > 0$ [Silverman 1994, p. 420]. We refer to the connected component of the identity as the *nose*. If there is a second component, we refer to it as the *egg*. For a curve with two components, let P_{egg}, Q_{egg} be points on the egg, and let P_{nose}, Q_{nose} be points on the nose. Then $P_{\text{egg}} + Q_{\text{egg}}$ and $P_{\text{nose}} + Q_{\text{nose}}$ are on the nose, while $P_{\text{egg}} + P_{\text{nose}} = P_{\text{nose}} + P_{\text{egg}}$ is on the egg.

Since our definition of the elliptic Fermat numbers involves doubling points, it is convenient to use the notation $2^k P = (m_k/e_k^2, n_k/e_k^3)$. We also rely on the *duplication formula* expressing the x-coordinate of $2Q$ in terms of that of Q. In particular, if $2^{k-1}P = (x_{k-1}, y_{k-1})$, [Silverman and Tate 1992, p. 39] gives

$$X(2^k P) = \frac{x_{k-1}^4 - 2bx_{k-1}^2 - 8cx_{k-1} + b^2 - 4ac}{4(x_{k-1}^3 + ax_{k-1}^2 + bx_{k-1} + c)}.$$

Letting $2^{k-1}P = (m_{k-1}/e_{k-1}^2, n_{k-1}/e_{k-1}^3)$, we can put this in terms of m_{k-1}, e_{k-1}, and n_{k-1}:

$$X(2^k P) = \frac{m_{k-1}^4 - 2bm_{k-1}^2 e_{k-1}^4 - 8cm_{k-1}e_{k-1}^6 + b^2 e_{k-1}^8 - 4ace_{k-1}^8}{4n_{k-1}^2 e_{k-1}^2}. \tag{6}$$

We will refer to the unreduced numerator and denominator in the above equation as A and B, respectively; i.e.,

$$A = m_{k-1}^4 - 2bm_{k-1}^2 e_{k-1}^4 - 8cm_{k-1}e_{k-1}^6 + b^2 e_{k-1}^8 - 4ace_{k-1}^8, \tag{7}$$

$$B = 4n_{k-1}^2 e_{k-1}^2. \tag{8}$$

One last aspect of elliptic curves that will prove useful in Section 7 is the concept of complex multiplication. We say that an elliptic curve has *complex multiplication* if its endomorphism ring is isomorphic to an order in an imaginary quadratic field. In other words, E is equipped with more maps than simple integer multiplication of a point, and composition of these maps is similar to multiplication in an imaginary quadratic field.

Complex multiplication is relevant to our work because it allows us to count the points on the curve over finite fields. In the final section, we will study the curve $E : y^2 = x^3 - 2x$, and our results rely on having a good understanding of $|E(\mathbb{F}_p)|$. As a special case of Proposition 8.5.1 from [Cohen 2007, p. 566], we have the following fact about our curve E:

Proposition 12. *Let $E : y^2 = x^3 - 2x$ be an elliptic curve and let p be an odd prime. Then $|E(\mathbb{F}_p)| = p + 1 - a_p(E)$, where $a_p(E)$ is known as the* ***trace of Frobenius*** *of an elliptic curve modulo p. When $p \equiv 3 \pmod 4$, we have $a_p(E) = 0$. If $p \equiv 1 \pmod 4$, then*

$$a_p(E) = 2\left(\frac{2}{p}\right) \begin{cases} -a, & \textit{if } 2^{(p-1)/4} \equiv 1 \pmod p, \\ a, & \textit{if } 2^{(p-1)/4} \equiv -1 \pmod p, \\ -b, & \textit{if } 2^{(p-1)/4} \equiv -a/b \pmod p, \\ b, & \textit{if } 2^{(p-1)/4} \equiv a/b \pmod p, \end{cases}$$

where a and b are integers such that $p = a^2 + b^2$ with $a \equiv -1 \pmod 4$.

3. Coprimality and order universality

We begin by proving Corollary 4 and then use this to prove Theorem 2, that is, $\gcd(F_k(E, P), F_\ell(E, P))$ can only be a multiple of primes of bad reduction.

Proof of Corollary 4. If $p \nmid \Delta(E)$, then p is a prime of good reduction for E. We have $p \mid F_k(E, P)$ if and only if $2^k P$ reduces modulo p to a nonsingular point with $y \equiv 0 \pmod p$. This occurs if and only if $2^{k+1} P \equiv (0:1:0) \pmod p$ and since $2^k P \not\equiv (0:1:0) \pmod p$ it follows that the order of $P \in E(\mathbb{F}_p)$ is 2^k. □

Now, we prove Theorem 2.

Proof. Suppose that p is a prime that divides $\gcd(F_k(E, P), F_\ell(E, P))$. If p is a prime of good reduction for E, the previous corollary gives that $p \mid F_k(E, P)$

implies that $P \in E(\mathbb{F}_p)$ must have order exactly 2^{k+1}, and $p \mid F_\ell(E, P)$ implies that $P \in E(\mathbb{F}_p)$ must have order exactly $2^{\ell+1}$. This is a contradiction if $k \neq \ell$. □

Note that the nonsingularity of E mod p is necessary in both of the proofs above. If $E : y^2 = x^3 + x^2 + 67x + 79$, then E is singular mod 43. The point $P = (10, 43) \in E(\mathbb{Q})$ has infinite order and $2P = \left(-\frac{3}{4}, \frac{43}{8}\right)$ has the property that P and $2P$ (and in fact $2^k P$ for all $k \geq 1$) reduce to a singular point modulo 43, because $P \notin E_0(\mathbb{Q}_{43})$ and the Tamagawa number of E at 43 is 3. It follows that $F_k(E, P)$ is a multiple of 43 for all k.

To embark on the proof of Theorem 3, we must make sense of reducing points on an elliptic curve modulo an arbitrary integer N, and for this reason we need to recall some results from the theory of elliptic curves over arbitrary rings. Our treatment comes from that of [Lenstra 1987a]. Given a commutative ring R, we say that a finite collection of elements (a_i) is *primitive* if it generates R as an R-ideal. That is, (a_i) is primitive if there exist $b_i \in R$ such that $\sum a_i b_i = 1$.

Lenstra showed that there is a natural way to define a group structure on the points on E in $\mathbb{P}^2(R)$ provided $6\Delta(E)$ is a unit in R, and for any primitive $m \times n$ matrix with entries in R whose 2×2 subdeterminants are all zero, there exists a linear combination of the rows that is primitive in R. This second condition holds in any finite ring and also in any PID, and so Lenstra's construction works in $\mathbb{Z}/N\mathbb{Z}$ if $\gcd(6\Delta(E), N) = 1$.

Given points $S = (x_1 : y_1 : z_1)$ and $T = (x_2 : y_2 : z_2)$ in $E(\mathbb{Z}/N\mathbb{Z})$, Lenstra described *three* families of polynomials in the six variables $(x_1, y_1, z_1, x_2, y_2, z_2)$ such that $S + T$ can be given by any of $(q_1 : r_1 : s_1)$, $(q_2 : r_2 : s_2)$, $(q_3 : r_3 : s_3)$, provided one of these points is primitive. Lenstra showed that the 3×3 matrix made with the polynomials as its entries has vanishing 2×2 subdeterminants, and is primitive. It follows that some linear combination $(q_0 : r_0 : s_0)$ of the rows gives a formula for $S + T$ in $E(\mathbb{Z}/N\mathbb{Z})$. This construction works not just over $\mathbb{Z}/N\mathbb{Z}$, but also over $R = \mathbb{Z}[1/(6|\Delta(E)|)]$ and gives E the structure of a group scheme over this ring. It follows from Proposition 3.2 of Chapter IV of [Silverman 1994] that the reduction map $E(R) \to E(\mathbb{Z}/N\mathbb{Z})$ is a homomorphism. By thinking of a point in $E(\mathbb{Q})$, namely $(m/e^2, n/e^3)$ as $(me : n : e^3) \in E(R)$, we get that the reduction mod N map $E(\mathbb{Q}) \to E(\mathbb{Z}/N\mathbb{Z})$ is a homomorphism. It is worth noting that $(m/e^2, n/e^3)$ reduces to $(0 : 1 : 0)$ modulo N if and only if $e \equiv 0 \pmod{N}$. From this, it follows that if $N = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, then the natural map

$$E(\mathbb{Z}/N\mathbb{Z}) \to \prod_{i=1}^{k} E(\mathbb{Z}/p_i^{e_i}\mathbb{Z})$$

is an isomorphism. Now we prove Theorem 3.

Proof. Let $P \in E(\mathbb{Q})$ be a point of infinite order and k a nonnegative integer. Recall that we define $2^k P = (m_k e_k : n_k : e_k^3)$ for $m_k, n_k, e_k \in \mathbb{Z}$ with $\gcd(m_k, e_k) =$

$\gcd(n_k, e_k) = 1$. We consider first the case where $N = p^r$ is an odd prime power. In that situation, we have that if $p^r \mid F_k(E, P)$, then $2^k P \equiv (x : 0 : 1) \pmod{p^r}$ and so the order of P in $E(\mathbb{Z}/p^r\mathbb{Z})$ is 2^{k+1}. Conversely, if the order of $P \in E(\mathbb{Z}/p^r\mathbb{Z})$ is 2^{k+1}, then e_{k+1} is a multiple of p^r. However, the duplication formula shows that $e_{k+1} \mid 2n_k e_k$. Since $2^k P = (m_k e_k : n_k : e_k^3)$ has order 2 in $E(\mathbb{Z}/p^r\mathbb{Z})$, it also has order 2 in $E(\mathbb{Z}/p\mathbb{Z})$ and so $p \mid n_k$, which implies that $p \nmid e_k$. Thus, $p^r \mid 2n_k e_k$ but $\gcd(p, e_k) = 1$ and so $p^r \mid n_k = F_k(E, P)$. Theorem 2 gives that $N \mid F_k(E, P)$ if and only if $N \mid F_0(E, P) F_1(E, P) \cdots F_k(E, P)$ but $N \nmid F_0(E, P) F_1(E, P) \cdots F_{k-1}(E, P)$. The desired result follows.

Now, we consider the general case. If $N = \prod_{i=1}^{\ell} p_i^{e_i}$, we have the isomorphism

$$E(\mathbb{Z}/N\mathbb{Z}) \cong \prod_{i=1}^{\ell} E(\mathbb{Z}/p_i^{e_i}\mathbb{Z}).$$

It follows from this that P has order equal to 2^{k+1} in $E(\mathbb{Z}/N\mathbb{Z})$ if and only if (i) for all prime powers $p_i^{e_i}$ the order of P in $E(\mathbb{Z}/p_i^{e_i}\mathbb{Z})$ is equal to 2^j for some $j \le k+1$, and (ii) there is a prime power $p_j^{e_j}$ such that $P \in E(\mathbb{Z}/p_j^{e_j}\mathbb{Z})$ is 2^{k+1}. Condition (i) means that $p_i^{e_i} \mid F_{j-1}(E, P)$ and condition (ii) means that $p_j^{e_j} \mid F_k(E, P)$ (and hence by Theorem 2 that $p_j \nmid F_\ell(E, P)$ for $\ell < k$). It follows that $P \in E(\mathbb{Z}/N\mathbb{Z})$ has order 2^{k+1} if and only if $N \mid F_0(E, P) \cdots F_k(E, P)$ but $N \nmid F_0(E, P) \cdots F_{k-1}(E, P)$. □

4. Recurrence

We will now explore the recurrence relation given by Theorem 5. Before continuing, we define the sequence $\{\tau_k\}$. If we write $2^{k-1}P = (m_{k-1}/e_{k-1}^2, F_{k-1}/e_{k-1}^3)$ with $m_{k-1}, F_{k-1}, e_{k-1} \in \mathbb{Z}$ with $e_{k-1} \ge 1$ and $\gcd(m_{k-1}, e_{k-1}) = \gcd(F_{k-1}, e_{k-1}) = 1$, then let

$$\tau_k(E, P) = \frac{2F_{k-1}e_{k-1}}{e_k}.$$

When the duplication formula is applied to compute the x-coordinate of $2^k P$, we obtain the formula

$$X(2^k P) = \frac{m_{k-1}^4 - 2bm_{k-1}^2 e_{k-1}^2 - 8cm_{k-1}e_{k-1}^6 + (b^2 - 4ac)e_{k-1}^8}{(2F_{k-1}e_{k-1})^2} = \frac{A}{B} = \frac{m_k}{e_k^2}.$$

Here $(2F_{k-1}e_{k-1})^2 = B$ is the "unreduced" denominator of $X(2^k P)$, and e_k^2 is the reduced denominator. So $e_k \mid 2F_{k-1}e_{k-1}$, and the number τ_k measures the discrepancy between the two quantities e_k and $2F_{k-1}e_{k-1}$, that is, the amount of cancellation that occurs. It is clear then that $\tau_k^2 = \gcd(A, B)$.

We will now prove Theorem 5. For now, keep in mind that we can explicitly calculate τ_k for all k; we will prove this at the end of the section. We can see that

(3) is just a restatement of the definition of τ_k and (1) is just a restatement of the duplication formula.

Lemma 13. *Equation (2) is correct.*

Proof. From the formulas given in [Silverman 1986, p. 58–59], we can see that

$$Y(2^k P) = \frac{1}{2F_{k-1}e_{k-1}^3 e_k^2}\big(-2am_{k-1}m_k e_{k-1}^4 - bm_{k-1}e_{k-1}^4 e_k^2 \\ -bm_k e_{k-1}^6 - 2ce_{k-1}^6 e_k^2 + m_{k-1}^3 e_k^2 - 3m_{k-1}^2 m_k e_{k-1}^2\big).$$

Then since $Y(2^k P) = F_k/e_k^3$,

$$\begin{aligned} F_k &= Y(2^k P)\cdot e_k^3 \\ &= \frac{1}{2F_{k-1}e_{k-1}^3}\big(-2am_{k-1}m_k e_{k-1}^4 e_k - bm_{k-1}e_{k-1}^4 e_k^3 \\ &\qquad -bm_k e_{k-1}^6 e_k - 2ce_{k-1}^6 e_k^3 + m_{k-1}^3 e_k^3 - 3m_{k-1}^2 m_k e_{k-1}^2 e_k\big). \end{aligned}$$

Then using the fact that $e_k/e_{k-1} = 2F_{k-1}/\tau_k$, we can simplify this to

$$F_k(E, P) = \frac{1}{\tau_k^3}\big(-2am_{k-1}m_k e_{k-1}^2 \tau^2 - 4bm_{k-1}e_{k-1}^4 F_{k-1}^2 \\ -bm_k e_{k-1}^4 \tau_k^2 - 8ce_{k-1}^6 F_{k-1}^2 + 4m_{k-1}^3 F_{k-1}^2 - 3m_{k-1}^2 m_k \tau_k^2\big). \quad \square$$

We can now see that the recurrence relation is correct, thus proving Theorem 5. The remainder of this section will be devoted to developing a better understanding of τ_k and developing an algorithm to calculate the sequence.

Ayad [1992] studied the sequences obtained by taking a point M on an elliptic curve, and evaluated the usual division polynomials at M to compute

$$mM = \left(\frac{\phi_m(M)}{\psi_m^2(M)}, \frac{\omega_m(M)}{\psi_m^3(M)}\right).$$

Ayad [1992, Théorème A] proved that if p is a prime, then there is an integer n such that $\phi_n(M)$ and $\psi_n(M)$ both have positive p-adic valuation if and only if M is singular modulo p, and moreover that in this case $\psi_m(M)$ is a multiple of P for all $m \geq 2$. As a consequence of this, it follows that the only primes that can divide τ_k are the primes of bad reduction. Also, applying Ayad's theorem with $M = 2^{k-1}P$, if p is an odd prime and $p \mid \tau_k$, then $2^{k-1}P$ is a singular point modulo p.

We next wish to obtain more precise information about the power of a prime of bad reduction that can divide τ_k. In particular, for $E : y^2 = x^3 + ax^2 + bx + c$, we define $\Delta(E) = 16(-4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2)$. The primes for which this model of E has bad reduction are precisely the primes that divide $\Delta(E)$. (We do not assume that $E : y^2 = x^3 + ax^2 + bx + c$ is a global minimal model for E.)

Lemma 14. *The number τ_k^2 divides $\frac{1}{4}\Delta(E)$.*

Proof. Let

$$\begin{aligned} f(x) &= x^3+ax^2+bx+c, \\ F(x) &= 3x^3-ax^2-5bx+2ab-27c, \\ \phi(x) &= x^4-2bx^2-8cx+b^2-4ac, \\ \Phi(x) &= -3x^2-2ax+a^2-4b. \end{aligned}$$

Silverman and Tate [1992, p. 62] showed that $\frac{1}{16}\Delta(E)=f(x)F(x)+\phi(x)\Phi(x)$. Setting $x=X(2^{k-1}P)$, we obtain

$$\begin{aligned} &\tfrac{1}{16}\Delta(E)e_{k-1}^{12} \\ &\quad= \left(e_{k-1}^{6}f\left(\frac{m_{k-1}}{e_{k-1}^{2}}\right)\right)\left(e_{k-1}^{6}F\left(\frac{m_{k-1}}{e_{k-1}^{2}}\right)\right)+\left(e_{k-1}^{4}\Phi\left(\frac{m_{k-1}}{e_{k-1}^{2}}\right)\right)\left(e_{k-1}^{8}\phi\left(\frac{m_{k-1}}{e_{k-1}^{2}}\right)\right). \end{aligned}$$

Recall that $\tau_k^2=\gcd(A,B)$ where A and B are given by (7) and (8). Rewriting this equation in terms of A and B gives

$$\tfrac{1}{16}\Delta(E)e_{k-1}^{12}=\frac{B}{4e_{k-1}^{2}}\left(e_{k-1}^{6}F\left(\frac{m_{k-1}}{e_{k-1}^{2}}\right)\right)+\left(e_{k-1}^{4}\Phi\left(\frac{m_{k-1}}{e_{k-1}^{2}}\right)\right)A.$$

Multiplying through by $4e_{k-1}^2$ gives that A and B both divide $\frac{1}{4}\Delta(E)e_{k-1}^{14}$. However, $\gcd(m_{k-1},e_{k-1})=1$ implies that $\gcd(A,e_{k-1})=1$ and so $\tau_k^2=\gcd(A,B)$ is relatively prime to e_{k-1} and so $\tau_k^2 \mid \left(\frac{1}{4}\Delta(E)\right)$, as desired. □

As stated above, Ayad's theorem implies that if $p\mid\tau_k$, then $2^{k-1}P$ is a singular point modulo p. We will prove a converse to this result.

Theorem 15. *Let p be an odd prime. Suppose that $2^{k-1}P$ and 2^kP both reduce to singular points mod p. Then $p\mid\tau_k$.*

Proof. Since p is odd, singular points modulo p have y-coordinate $\equiv 0 \pmod p$ and hence if $2^{k-1}P$ reduces to a singular point modulo p, then $p\mid F_{k-1}(E,P)$. On the other hand, 2^kP reducing to a singular point modulo p means that $p\nmid e_k$ and hence $p\mid\tau_k=2F_{k-1}e_{k-1}/e_k$. □

The results above apply for odd primes. Now, we consider the parity of τ_k and F_k.

Theorem 16. *If* $2^kP\not\equiv(0:1:0) \pmod 2$, *then τ_k is even. If* $2^{k-1}P\equiv 2^kP\equiv (0:1:0) \pmod 2$, *then τ_k is odd.*

Proof. If $2^kP\not\equiv(0:1:0)\pmod 2$, then $2\nmid e_k$. Since $\tau_k(E,P)=2F_{k-1}e_{k-1}/e_k$, the numerator is even and the denominator is odd, so τ_k is even.

If $2^{k-1}P \equiv 2^k P \equiv (0:1:0) \pmod 2$, then e_{k-1} and e_k are both even, while m_{k-1} and m_k are both odd. Considering the duplication formula

$$\frac{A}{B} = \frac{m_{k-1}^4 - 2bm_{k-1}^2 e_{k-1}^2 - 8cm_{k-1}e_{k-1}^4 + (b^2-4ac)e_{k-1}^4}{(2F_{k-1}e_{k-1})^2},$$

one sees that A is odd and B is even, and since $\tau_k^2 = \gcd(A, B)$, it follows that τ_k is odd. □

Recalling that $E_1(\mathbb{Q}_p)$ denotes the set of points in $E(\mathbb{Q}_p)$ that reduce to the point at infinity modulo p, the above theorem gives that τ_k is even for all sufficiently large k if and only if the order of $P \in E(\mathbb{Q}_2)/E_1(\mathbb{Q}_2)$ is not a power of 2, and τ_k is odd for all sufficiently large k if and only if the order of $P \in E(\mathbb{Q}_2)/E_1(\mathbb{Q}_2)$ is a power of 2.

While it is nice to know all of these properties, we need to know exactly what τ_k is in order for the recurrence relations to be useful. In accordance with Theorem 6, we can calculate $|\tau_k|$ for all k using the following algorithm. (The proof of the correctness of the algorithm will be given later in this section.)

(1) Find and factor the discriminant $\Delta(E)$.

(2) For each prime p such that $p^2 \mid \Delta(E)$, complete the following:

(a) Find the smallest $\ell \in \mathbb{Z}^+$ such that $\ell P \equiv (0:1:0) \pmod p$.

(b) If ℓ is a power of 2, then $\operatorname{ord}_p(\tau_k) = 0$ for all $k \geq \ell + 1$.

(i) Move on to the next $p^2 \mid \Delta(E)$.

(c) If ℓ is not a power of 2, then $\operatorname{ord}_p(\tau_k) = \operatorname{ord}_p(2F_{k-1})$.

(i) Find some $r \in \mathbb{Z}^+$ such that $rP = (m/e^2, n/e^3)$ with $p^s \mid e$. Choose s such that either $p^{2s} \mid\mid \Delta(E)$ or $p^{2s+1} \mid\mid \Delta(E)$. Here $p^n \mid\mid a$ means that the prime power p^n fully divides a; that is, $p^n \mid a$ but $p^{n+1} \nmid a$.

(ii) Now $\operatorname{ord}_p(Y(tP))$ depends only on $t \bmod r$. Find all possible values of $2^k \bmod r$ and note the lowest k which generates each value.

(iii) Calculate $\operatorname{ord}_p(F_{k-1})$ for each k noted in (ii). Use this to calculate $\operatorname{ord}_p(\tau_k)$.

(iv) Move on to the next $p^2 \mid \Delta(E)$.

(3) We now know $\operatorname{ord}_p(\tau_k)$ for all (but finitely many, in some cases) k for each p such that $p^2 \mid \Delta(E)$, which are all the p that could divide τ_k. Use this to calculate $|\tau_k|$.

Note that doing the above computations in $E(\mathbb{Q})$ can be challenging since the heights of points on elliptic curves grow quickly. Instead, doing the computations in $E(\mathbb{Q}_p)$, which is implemented in Sage [SageMath 2017], is more straightforward.

Now we will prove that this algorithm is correct. In order to do this, we must first prove the following theorem.

Theorem 17. *Let $E : y^2 = x^3 + ax^2 + bx + c$ be an elliptic curve. Assume $Q, R \in E(\mathbb{Q})$ are such that*

$$Q = (x_1, y_1) = \left(\frac{m_1}{e_1^2}, \frac{n_1}{e_1^3}\right), \quad p \nmid e_1,$$
$$R = (x_2, y_2) = \left(\frac{m_2}{e_2^2}, \frac{n_2}{e_2^3}\right), \quad p^k \,||\, e_2.$$

Let

$$Q + R = (x_3, y_3) = \left(\frac{m_3}{e_3^2}, \frac{n_3}{e_3^3}\right).$$

Then

$$X(Q+R) \equiv X(Q) \pmod{p^k}, \quad Y(Q+R) \equiv Y(Q) \pmod{p^k}.$$

The result above follows from the fact that the natural map from $E(\mathbb{Q}) \to E(\mathbb{Z}/p^k\mathbb{Z})$ is a homomorphism in the case when $p \nmid 6\Delta(E)$, but in light of the algorithm above, we are primarily interested in the case where $p \mid 6\Delta(E)$.

Proof. From [Silverman 1986, p. 58–59], we know that if we let

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \quad \text{and} \quad v = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1},$$

then we have

$$x_3 = \lambda^2 - a - x_1 - x_2 = \frac{ax_2^2 + bx_2 + c - 2y_1y_2 + y_1^2 + 2x_1x_2^2 - x_1^2x_2}{x_2^2 - 2x_1x_2 + x_1^2} - a - x_1.$$

Now since $p^k \,||\, e_2$, we can let $x_2 = \tilde{x}_2 p^{-2k}$ and $y_2 = \tilde{y}_2 p^{-3k}$. Plugging this in yields

$$x_3 = \frac{a\tilde{x}_2^2 + b\tilde{x}_2p^{2k} + cp^{4k} - 2y_1\tilde{y}_2p^k + y_1^2p^{4k} + 2x_1\tilde{x}_2^2 - x_1^2\tilde{x}_2p^{2k}}{\tilde{x}_2^2 - 2x_1\tilde{x}_2p^{2k} + x_1^2p^{4k}} - a - x_1. \tag{9}$$

Reducing mod p^k and mod p^{2k} gives us

$$x_3 \equiv x_1 \pmod{p^k}, \tag{10}$$
$$x_3 \equiv x_1 - \frac{2y_1\tilde{y}_2p^k}{\tilde{x}_2^2} \pmod{p^{2k}}. \tag{11}$$

Now that we have shown that $x_3 \equiv x_1 \pmod{p^k}$, we just need to show that $y_3 \equiv y_1 \pmod{p^k}$. Since $x_3 \equiv x_1 \pmod{p^k}$, we can write $x_3 = x_1 + rp^k$. And again using the definitions of λ and v given above, we have

$$y_3 = -\lambda x_3 - v = \frac{-n_1m_1e_2^3 + n_1m_2e_1^2e_2 - n_1e_1^2e_2^3rp^k + n_2e_1^5rp^k}{m_1e_1^3e_2^3 - m_2e_1^5e_2}.$$

Once again, since $p^k \,||\, e_2$, we can let $e_2 = \tilde{e}_2 p^k$. Then

$$y_3 = \frac{-n_1 m_1 \tilde{e}_2^3 p^{2k} + n_1 m_2 e_1^2 \tilde{e}_2 - n_1 e_1^2 \tilde{e}_2^3 r p^{3k} + n_2 e_1^5 r}{m_1 e_1^3 \tilde{e}_2^3 p^{2k} - m_2 e_1^5 \tilde{e}_2}.$$

Reducing mod p^k gives us

$$y_3 \equiv \frac{-n_1}{e_1^3} - \frac{n_2 r}{m_2 \tilde{e}_2} \pmod{p^k}. \tag{12}$$

Now from (11), we know

$$r \equiv -\frac{2y_1\tilde{y}_2}{\tilde{x}_2^2} \pmod{p^k}.$$

Simple algebra allows us to see that

$$r \equiv \frac{-2n_1 n_2 \tilde{e}_2}{m_2^2 e_1^3} \pmod{p^k}.$$

Plugging this into (12), we get

$$\begin{aligned} y_3 &\equiv \frac{-n_1}{e_1^3} - \frac{n_2}{m_2\tilde{e}_2} \cdot \frac{-2n_1 n_2 \tilde{e}_2}{m_2^2 e_1^3} \pmod{p^k} \\ &\equiv \frac{-n_1}{e_1^3} + \frac{2n_1(m_2^3 + a m_2^2 e_2^2 + b m e_2^4 + c e_2^6)}{m_2^3 e_1^3} \pmod{p^k}. \end{aligned}$$

And since $e_2 \equiv 0 \pmod{p^k}$, we have

$$y_3 \equiv \frac{-n_1}{e_1^3} + \frac{2n_1 m_2^3}{m_2^3 e_1^3} \pmod{p^k} \equiv y_1 \pmod{p^k}, \tag{13}$$

completing the proof. □

Now we prove that the algorithm to calculate τ_k is correct.

Proof. From Lemma 14, we can conclude that for any p dividing τ_k, we must have $p^2 \mid \Delta(E)$. So we only need to consider primes p which satisfy this condition. We now break this problem into two cases based on the smallest $\ell \in \mathbb{Z}^+$ so that $\ell P \equiv (0:1:0) \pmod{p}$.

Case I: If ℓ is a power of 2, then there exists $d \in \mathbb{Z}^+$ such that $2^d P \equiv (0:1:0) \pmod{p}$. First, if $p > 2$, then for $k \geq d+1$, we have $p \nmid F_k$ and since e_k is a multiple of e_{k-1}, but e_k is a divisor of $2F_{k-1}e_{k-1}$, it follows that $\mathrm{ord}_p(e_{k-1}) = \mathrm{ord}_p(e_k)$ and so $p \nmid \tau_k$. If $p = 2$, the desired result follows from Theorem 16.

Case II: If ℓ is not a power of 2, then $2^k P \not\equiv (0:1:0) \pmod{p}$ for any k. This implies that $p \nmid e_k$ for any k and hence $\mathrm{ord}_p(\tau_k) = \mathrm{ord}_p(2F_{k-1})$. Choose s such that either $p^{2s} \,||\, \Delta(E)$ or $p^{2s+1} \,||\, \Delta(E)$. Now, we can find some $r \in \mathbb{Z}^+$ such that

$rP = (m/e^2, n/e^3)$ with $p^s \mid e$. Then $rP \equiv (0:1:0) \pmod{p^s}$. Using Theorem 17, we can see that $jP + rP \equiv jP \pmod{p^s}$ and conclude that $\operatorname{ord}_p(Y(tP))$ depends only on $t \bmod r$. Then, since $2^k \bmod r$ will repeat, we can use a finite number of calculations to determine $\operatorname{ord}_p(Y(2^k P)) = \operatorname{ord}_p(F_k)$ for all $k \geq 1$. □

5. Primality

In this section, we prove Theorem 7. This theorem states the following. Suppose that $E: y^2 = x^3 + ax^2 + bx$ is an elliptic curve of rank 1 generated by P with x-coordinate m_0/e_0^2 and the torsion subgroup of $E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ generated by $T = (0, 0)$, which lies on the egg and is the only integral point on the egg. Let $F_k(E, P)$ denote the sequence of elliptic Fermat numbers. Suppose that $\gcd(b, m_0) = 1$, and suppose that the Thue equation $x^4 + ax^2y^2 + by^4 = \pm 1$ has no integer solutions with $y \notin \{0, \pm 1\}$. Then all the elliptic Fermat numbers $F_k(E, P)$ are composite.

We start by proving two lemmas that will be useful in the proof of Theorem 7.

Lemma 18. *Assume that $E(\mathbb{Q}) \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $E(\mathbb{Q}) = \langle P, T \rangle$, where P is a generator of $E(\mathbb{Q})$ and T is a rational point of order 2. Assume that:*

(i) *E has an egg.*

(ii) *T is on the egg.*

(iii) *T is the only integral point on the egg.*

(iv) *P is not integral.*

Then T is the only integral point on E.

Proof. Every point in $E(\mathbb{Q})$ is of the form mP or $mP + T$. If P is on the nose, then we have that for any $m \neq 0$, mP is on the nose, and mP is not integral because P is not integral. We also have that $mP + T$ is on the egg and thus is not integral because T is the only integral point on the egg by assumption. If P is on the egg, then let $P' = P + T$. Then P' is on the nose, and the proof is the same as before. □

Lemma 19. *Let E be an elliptic curve of the form $y^2 = x^3 + ax^2 + bx$ and suppose* $\gcd(m_0, b) = 1$. *Then* $\gcd(m_k, b) = 1$ *for all k.*

Proof. We use induction. The base case $\gcd(m_0, b) = 1$ is true by assumption. Now assume that $\gcd(m_{k-1}, b) = 1$. Since $c = 0$, from our recurrence relations, we can see that

$$m_k = \frac{m_{k-1}^4 - 2bm_{k-1}^2 e_{k-1}^4 + b^2 e_{k-1}^8}{\tau_k^2}.$$

Now since b divides the terms $-2bm_{k-1}^2 e_{k-1}^4$ and $b^2 e_{k-1}^8$ in the numerator but is coprime to the term m_{k-1}^4, we know b is coprime to the numerator. Dividing by τ_k^2 will not change this. Thus $\gcd(m_k, b) = 1$ for all k. □

With these two lemmas, we can now prove Theorem 7.

Proof of Theorem 7. Let $2^k P = (m_k/e_k^2, F_k/e_k^3)$ and let $2^k P + T = (m_T/e_T^2, n_T/e_T^3)$. Using the formulas for adding points given in [Silverman 1986, p. 58–59], we see

$$X(2^k P + T) = \frac{be_k^2}{m_k}, \quad Y(2^k P + T) = \frac{-bF_k e_k}{m_k^2}. \tag{14}$$

By the assumption that $\gcd(b, m_0) = 1$ and by Lemma 19, we know $\gcd(b, m_k) = 1$. And since $\gcd(m_k, e_k) = 1$, the first equation in (14) must be in lowest terms. This gives $e_T = \sqrt{|m_k|}$ and $n_T = -bF_k e_k/\sqrt{|m_k|}$. We find from this that

$$-\frac{n_T e_T}{be_k} = \frac{(bF_k e_k/\sqrt{|m_k|})\sqrt{|m_k|}}{be_k} = F_k.$$

Note that if p is a prime and $p \mid e_k$ then $2^k P \equiv (0:1:0) \pmod p$, in which case $2^k P + T \equiv T \pmod p$. And since T is not the point at infinity, $2^{k-1} P + T \not\equiv (0:1:0) \pmod p$. Therefore $p \nmid e_T$. Hence $\gcd(e_k, e_T) = 1$. Since $e_T = \sqrt{|m_k|}$ and $\gcd(b, m_k) = 1$, we get the factorization

$$F_k = \left(-\frac{n_T}{be_k}\right) e_T,$$

where both factors are integers. Therefore F_k is composite as long as

$$\frac{n_T}{be_k} = -\frac{F_k}{\sqrt{|m_k|}} \neq \pm 1.$$

If we assume that $F_k = \pm\sqrt{|m_k|}$, then $2^k P = (m_k/e_k^2, F_k/e_k^3)$ being a point on E gives $|m_k| = F_k^2 = m_k^3 + am_k^2 e_k^2 + bm_k e_k^4$, which yields $m_k^2 + am_k e_k^2 + be_k^4 = \pm 1$. But by assumption, this equation has no solutions where $e_k \notin \{0, \pm 1\}$. Therefore F_k is composite for all $k \geq 1$. □

6. Growth rate

In this section, we will discuss the growth rate of the elliptic Fermat numbers and prove Theorem 8. In order to do so, we need a few more tools. The first new definition we need is the *height* of a point.

Definition 20. The *height* of a point $P = (m/e^2, n/e^3)$ on an elliptic curve is defined as

$$h(P) = \log(\max(|m|, e^2)).$$

The height of a point gives us a way to express how “complicated” the coordinates of the point are. We also need to make use of the *canonical height*.

Definition 21. The *canonical height* of a point P on an elliptic curve is defined as

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

Note that Theorem 8 can be summarized as saying that F_k is approximately equal to $e^{4^k\cdot(3/2)\hat{h}(P)}$. So the elliptic Fermat sequences grow doubly exponentially, like the classic Fermat sequence, albeit much more quickly. The proof is as follows:

Proof of Theorem 8. First, recall that $|F_k| = |\tau_{k+1}|e_{k+1}/(2e_k)$. This relates the y-coordinate of $2^k P$ to the x-coordinate. We then have

$$\begin{aligned}\lim_{k\to\infty} \frac{\log(|F_k(E, P)|)}{4^k} &= \lim_{k\to\infty} \frac{\log(|\tau_{k+1}|e_{k+1}/(2e_k))}{4^k} \\ &= \lim_{k\to\infty} \frac{\frac{1}{2}\log(e_{k+1}^2)}{4^k} - \lim_{k\to\infty} \frac{\frac{1}{2}\log(e_k^2)}{4^k} + \lim_{k\to\infty} \frac{\log\left(\frac{1}{2}|\tau_{k+1}|\right)}{4^k} \\ &= 2\lim_{k\to\infty} \frac{\log(e_{k+1}^2)}{4^{k+1}} - \tfrac{1}{2}\lim_{k\to\infty} \frac{\log(e_k^2)}{4^k} + 0 \\ &= 2\hat{h}(P) - \tfrac{1}{2}\hat{h}(P) = \tfrac{3}{2}\hat{h}(P). \qquad \square\end{aligned}$$

7. Elliptic Fermat numbers for the curve $y^2 = x^3 - 2x$

In this section, we apply the hitherto developed theory of elliptic Fermat numbers to examine properties of the curve $E : y^2 = x^3 - 2x$ and the point $P = (2, 2) \in E(\mathbb{Q})$.

We begin with some remarks on E and the point P. Recall that E is equipped with complex multiplication and so Proposition 12 gives a formula for $|E(\mathbb{F}_p)|$ for all p. Elliptic curves with complex multiplication are the key to the elliptic curve primality proving algorithm of Atkin, Goldwasser, Kilian and Morain, and elliptic curve algorithms to prove primality of Fermat numbers and other special sequences have been considered previously in [Gross 2005; Denomme and Savin 2008; Tsumura 2011; Abatzoglou et al. 2016]. The last remark we make is about the elliptic Fermat sequence $\{F_n(E, P)\}$ and the appearance of Fermat primes and Mersenne primes, i.e, primes of the form $2^p - 1$ for a prime p, in the factorization of $F_k(E, P)$.

Table 1 provides factorizations of the first five elliptic Fermat numbers for E at P, with known Fermat and Mersenne primes in bold. (The primes p_6, p_7 have 16 digits each, and p_8 and p_9 have 18 digits each.) In fact, every odd prime factor dividing $F_n(E, P)$ for $n \geq 2$ will have a congruence that is either Mersenne-like or Fermat-like. We now present the proof of Theorem 9, beginning with the congruence result for a prime divisor $p \equiv -1 \pmod 4$, which yields a tidy Mersenne-like congruence.

Proof of Theorem 9 for $p \equiv 3 \pmod 4$. By Theorem 3, $p \mid F_n(E, P)$ tells us that P has order 2^{n+1} in $E(\mathbb{F}_p)$. Then by Lagrange's theorem and Proposition 12, $2^{n+1} \mid |E(\mathbb{F}_p)| = p + 1$, and so $p \equiv -1 \pmod{2^{n+1}}$. □

n	$F_n(E, P)$
0	2
1	$-\mathbf{3}\cdot\mathbf{7}$
2	$\mathbf{31}\cdot 113\cdot\mathbf{257}$
3	$-2113\cdot 2593\cdot 46271\cdot 101281\cdot 623013889$
4	$\mathbf{127}\cdot\mathbf{65537}\cdot 33303551\cdot 70639871\cdot 364024274689\cdot p_6\cdot p_7\cdot p_8\cdot p_9$

Table 1. Factorizations of the first five elliptic Fermat numbers for E at P.

Proving the congruence in the case of a prime divisor of an elliptic Fermat number congruent to 1 modulo 4 will require multiple steps. We will eventually show that such a prime divisor of $F_n(E, P)$ is congruent to 1 modulo 2^n, but we begin by showing an initial congruence result:

Lemma 22. *Let $E : y^2 = x^3 - 2x$ be an elliptic curve, $P = (2, 2)$ a point of infinite order and $F_n(E, P)$ the n-th elliptic Fermat number associated to E at the point P. Then for any odd prime divisor $p \equiv 1 \pmod 4$ of $F_n(E, P)$, $n \geq 3$, we have $p \equiv 1 \pmod{\max(2^{\lfloor (n+1)/2\rfloor}, 8)}$.*

Proof. If $p \equiv 1 \pmod 4$, then $p = a^2 + b^2$, where $a \equiv -1 \pmod 4$. Recall that Proposition 12 gives a formula for the value of $|E(\mathbb{F}_p)|$ which depends on the quartic character of 2 modulo p. Let us first consider the case where 2 is a fourth power. Then $|E(\mathbb{F}_p)| = p + 1 - 2a$.

Like the proof of the previous theorem, we use Lagrange's theorem to show that $2^{n+1} \mid E(\mathbb{F}_p) = a^2 + b^2 + 1 - 2a = (a-1)^2 + b^2$. So $(a-1)^2 + b^2 \equiv 0 \pmod{2^{n+1}}$. Then $a - 1 \equiv b \equiv 0 \pmod{2^{\lfloor (n+1)/2\rfloor}}$, giving $p = a^2 + b^2 \equiv 1^2 + 0^2 \pmod{2^{\lfloor (n+1)/2\rfloor}}$. A symmetric argument follows when 2 is a quadratic residue but not a fourth power. In this situation we arrive at the equation $(a+1)^2 + b^2 \equiv 0 \pmod{2^{n+1}}$; however, the result is precisely the same.

To conclude, we rule out the case where 2 is not a quadratic residue modulo p. This would imply $|E(\mathbb{F}_p)| = p + 1 \pm 2b$. The same algebraic manipulation leads to a similar situation where $a^2 + (b \mp 1)^2 \equiv 0 \pmod{2^{n+1}}$, but this means $b \equiv \pm 1 \pmod{2^{\lfloor (n+1)/2\rfloor}}$; however, b is the even part of the two-square representation of p. So it cannot be the case that 2 is not a quadratic residue modulo 8, which happens only when $p \equiv 5 \pmod 8$. □

Because of the lemma, we have $p \equiv 1 \pmod 8$, and so we can make sense of $\sqrt{2}$ and i modulo p. We now define the recklessly notated action i on $E(\mathbb{F}_p)$ as $i(x, y) \mapsto (-x, iy)$, where the point $(-x, iy)$ uses i as the square root of -1 modulo p. This action makes $E(\mathbb{F}_p)$ into a $\mathbb{Z}[i]$-module. We will prove one last lemma concerning the action of $(1 + i)$ before moving on to the full congruence.

Lemma 23. *Let $E : y^2 = x^3 - 2x$ be an elliptic curve, $P = (2, 2)$ a point of infinite order and $F_n(E, P)$ the n-th elliptic Fermat number associated to E at the point P. Then for any odd prime factor $p \equiv 1 \pmod 4$ of $F_n(E, P)$, $n \geq 3$, we have $(1+i)^{2n+2}P = 0$ in $E(\mathbb{F}_p)$ and $(1+i)^{2n}P \neq 0$.*

Proof. Note that $(1+i)^k P = 2^k i^k P$. Recall that P has order 2^{n+1}, so

$$(1+i)^{2(n+1)}P = (2i)^{n+1}P = i^{n+1}(2^{n+1}P) = i^{n+1} \cdot 0 = 0.$$

It suffices to show that $(1+i)^x P \neq 0$ for $x \leq 2n$. Suppose not, and $(1+i)^x P = 0$. Then certainly $(1+i)^{2n}P = i^n 2^n P = 0$. The action of i^{n-1} makes no difference on the identity. This implies that $2^n P = 0$, contradicting order universality since P has order 2^{n+1}. □

With this last lemma proven, we are ready to introduce the Fermat-like congruence in full regalia and finish Theorem 9.

Proof of Theorem 9 for $p \equiv 1 \pmod 4$. As a consequence of the lemma above, we have that either $(1+i)^{2n+2}P = 0$ or $(1+i)^{2n+1}P = 0$. We are able to bolster the $(2n+1)$-case by introducing a new point $Q = (-i(\sqrt{2}-2), (2-2i)(\sqrt{2}-1))$. It is routine point addition to see that $(1+i)Q = (2, 2) = P$. In either case we have $(1+i)^{2n+3}Q = 0$ and $(1+i)^{2n+1}Q \neq 0$.

Consider the $\mathbb{Z}[i]$-module homomorphism $\phi : \mathbb{Z}[i] \to E(\mathbb{F}_p)$ given by $\phi(x) = xQ$. The image of ϕ is $\mathbb{Z}[i]Q = \{(a+bi)Q \mid a, b \in \mathbb{Z}\}$, the orbit of $\mathbb{Z}[i]$ on Q. By the first isomorphism theorem, $\mathbb{Z}[i]Q$ is isomorphic to $\mathbb{Z}[i]/\ker(\phi)$. Since $(1+i)^{2n+1} \notin \ker(\phi)$ and $(1+i)^{2n+3} \in \ker(\phi)$, and $(1+i)$ is an irreducible ideal in $\mathbb{Z}[i]$, we know the kernel is either the ideal $((1+i)^{2n+2})$ or $((1+i)^{2n+3})$; hence $\mathbb{Z}[i]/\ker(\phi)$ is a group of size 2^k, where $k = 2n+2$ or $k = 2n+3$.

Like the previous congruence results, we use Lagrange's theorem to assert $2^k \mid |E(\mathbb{F}_p)|$ and through the same reasoning as before, we arrive at

$$p \equiv 1 \pmod{2^{\lfloor k/2 \rfloor} = 2^{n+1}}.$$ □

We now present the proofs of Theorems 10 and 11, which give us information about sufficiently large Fermat and Mersenne primes dividing the elliptic Fermat sequence $\{F_n(E, P)\}$. First, we provide two lemmas.

Lemma 24. *Let $p \equiv \pm 1 \pmod{2^n}$ be an odd prime. Let ζ_ℓ denote a primitive ℓ-th root of unity in some extension of $\mathbb{F}_p$. Then $\zeta_{2^k} + \zeta_{2^k}^{-1}$ exists in $\mathbb{F}_p$ for all $k \leq n$.*

Proof. If $p \equiv 1 \pmod{2^k}$, then clearly there is a primitive 2^k-th root of unity in $\mathbb{F}_p$.

If $p \equiv 3 \pmod 4$, then we employ methods from Galois theory. First, because $p \equiv -1 \pmod{2^k}$, we have $p^2 \equiv 1 \pmod{2^k}$. Then there is a primitive 2^k-th root of unity in $\mathbb{F}_{p^2}$. Then we have that $\alpha = \zeta_{2^k} + \zeta_{2^k}^{-1}$ is in $\mathbb{F}_p$ if and only if $\sigma(\alpha) = \alpha$, where $\sigma(x) = x^p$ is the Frobenius endomorphism.

This says that $\alpha \in \mathbb{F}_p$ if and only if

$$\alpha^p = (\zeta_{2^k} + \zeta_{2^k}^{-1})^p = \zeta_{2^k}^p + \zeta_{2^k}^{-p} = \zeta_{2^k} + \zeta_{2^k}^{-1}.$$

We may write this equality as $\zeta_{2^k}^{2p} + \zeta_{2^k}^{p+1} + \zeta_{2^k}^{-p+1} + 1 = 0$. This factors into $(\zeta_{2^k}^p - \zeta_{2^k})(\zeta_{2^k}^p - \zeta_{2^k}^{-1}) = 0$. Then the equality holds if and only if $\zeta_{2^k}^p = \zeta_{2^k}$, meaning $p \equiv 1 \pmod{2^k}$, or $\zeta_{2^k}^p = \zeta_{2^k}^{-1}$; hence $p \equiv -1 \pmod{2^k}$. □

Lemma 25. *Let p be a Fermat or Mersenne prime that is at least* 31. *Then there exists a $Q \in E(\mathbb{F}_p)$ such that $2Q = P$.*

Proof. From [Silverman and Tate 1992, p. 76], for E we have its isogenous curve $E' : y^2 = x^3 + 8x$ and two homomorphisms, $\phi : E \to E'$ and $\psi : E' \to E$ given by

$$\phi(x, y) = \begin{cases} \left(\dfrac{y^2}{x^2}, \dfrac{y(x^2+2)}{x^2}\right) & \text{if } (x, y) \neq (0:0:1), (0:1:0), \\ (0:1:0) & \text{otherwise,} \end{cases}$$

$$\psi(x, y) = \begin{cases} \left(\dfrac{y^2}{4x^2}, \dfrac{y(x^2-8)}{8x^2}\right) & \text{if } (x, y) \neq (0:0:1), (0:1:0), \\ (0:1:0) & \text{otherwise.} \end{cases}$$

The maps hold the special property $\phi \circ \psi(S) = 2S$. The advantage of this framework is that we are able to break point-halving, a degree-4 affair, into solving two degree-2 problems. Another fact from [Silverman and Tate 1992, p. 85] is that $P = (x, y) \in \psi(E'(\mathbb{Q}))$ if and only if x is a square.

We now use this to show there is a $Q \in E(\mathbb{F}_p)$ such that $2Q = P$. For brevity, let $z = \sqrt{2+\sqrt{2}}$, and we define the following ascending chain of fields: $\mathbb{Q}$, $K = \mathbb{Q}(\sqrt{2})$ and $L = K(z)$. Here K is the minimal subfield where P has a ψ preimage Q_1 in E', and L is the minimal subfield where that preimage has its own ϕ preimage Q in E. It is a quick check in Magma to verify that in $E(L)$, P is divisible by 2. It then remains to verify that the elements $\sqrt{2}$ and $z = \sqrt{2+\sqrt{2}}$ are in $\mathbb{F}_p$.

First, we have that since 2 has order p, which is odd, there exists $h_k \in \mathbb{F}_p^\times$ such that $(h_k)^{2^k} = 2$. So any 2-power root of 2 is sure to exist.

For $z = \sqrt{2+\sqrt{2}}$ itself, we use Lemma 24 and $p \equiv \pm 1 \pmod{16}$ to show that we have an element $z = \zeta_{16} + \zeta_{16}^{-1} \in \mathbb{F}_p$, so we have all the necessary elements of L in $E(\mathbb{F}_p)$ to show there exists a $Q \in E(\mathbb{F}_p)$ such that $2Q = P$. □

These two lemmas will allow us to sharpen the threshold to search for Fermat and Mersenne primes in the elliptic Fermat sequence. We now prove Theorem 10.

Proof. First, it is a quick computation in Magma to verify that for $p = 5, 17$, P does not have a 2-power order in $E(\mathbb{F}_p)$, and so by Corollary 4, we have that 5 and 17 do not divide any elliptic Fermat number generated by P.

We rely on Proposition 12 and Lagrange's theorem. For a classical Fermat prime $F_n \neq 5, 17$, we have that 2 is a fourth power in $\mathbb{Z}/F_n\mathbb{Z}$. We can see this because for a generator g of $\mathbb{Z}/F_n\mathbb{Z}$, we have $2 = g^k$, additionally, we have $g^{p-1} = g^{2^{2^n}} = 1$. We will show that $k \equiv 0 \pmod 4$. This is because 2 has order $2^{n+1} \in (\mathbb{Z}/F_n\mathbb{Z})^\times$, and so $2^{2^{n+1}} = (g^k)^{2^{n+1}} = 1$. Therefore, $2^{2^n} \mid k(2^{n+1})$, finally giving $2^{2^n-n-1} \mid k$, which is a multiple of 4 for $n \geq 3$.

Since 2 is a fourth power in $\mathbb{F}_p$, we know that $E : y^2 = x^3 - 2x$ is isomorphic to the curve $E' : y^2 = x^3 - x$. From [Denomme and Savin 2008], we also have $E'(\mathbb{F}_p) \cong \mathbb{Z}[i]/(1+i)^{2^n}$. Moreover, $\mathbb{Z}[i]/(1+i)^{2^n} = \mathbb{Z}[i]/2^{2^{n-1}} \cong (\mathbb{Z}/2^{2^{n-1}}\mathbb{Z}) \times (\mathbb{Z}/2^{2^{n-1}}\mathbb{Z})$, from which we can deduce that $E(\mathbb{F}_p) \cong (\mathbb{Z}/2^{2^{n-1}}\mathbb{Z}) \times (\mathbb{Z}/2^{2^{n-1}}\mathbb{Z})$. Thus the order of P is a divisor of $2^{2^{n-1}}$.

By Lemma 25, we know there exists some $Q \in E(\mathbb{F}_p)$ such that $2Q = P$. In light of this we can tighten this initial upper bound by noting that all elements have order dividing $2^{2^{n-1}}$, and so $2^{2^{n-1}-1}P = 2^{2^{n-1}-1}(2Q) = 2^{2^{n-1}}Q = 0$. We conclude that P has order dividing $2^{2^{n-1}-1}$ and so p must divide $F_k(E, P)$ for some $k \leq 2^{n-1} - 2$ by Corollary 4. □

It remains to discuss the appearance of a Mersenne prime in the elliptic Fermat sequence. We prove Theorem 11.

Proof. The method we take to show this bound begins with the fact that $|E(\mathbb{F}_q)| = q + 1 = 2^p$. Additionally, we have $E(\mathbb{F}_q) \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mn\mathbb{Z}$, where $q \equiv 1 \pmod m$. We have that $E(\mathbb{F}_q)$ contains all three points of order 2 because these are $(0, 0)$ and $(\pm\sqrt{2}, 0)$ and $\sqrt{2} \in \mathbb{F}_q$ since $q \equiv 7 \pmod 8$. Combining this with $q \equiv -1 \pmod{2^p}$ we have $E(\mathbb{F}_q) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{p-1}\mathbb{Z}$. So the order of any point in $E(\mathbb{F}_p)$ must divide 2^{p-1}. It suffices to exhibit a point R such that $4R = P$, so that $2^{p-3}P = 2^{p-3}2^2R = 2^{p-1}R = 0$.

Continuing the methodology first used in the proof of Lemma 25, we will show that such an R is in $E(\mathbb{F}_q)$ so that $2R = Q$, where $Q \in E(L)$ is the point found in Lemma 25 . To do this, we extend the fields from Lemma 25 and create

$$M = L(\sqrt{z(2+z)}) \quad \text{and} \quad N = M(\sqrt{\sqrt{2}(z-1)}).$$

Again, one may check in Magma that indeed P is divisible by 4 in $E(N)$, so we just need to check for the existence of necessary elements.

We have already shown there is an element z such that $z^2 = 2 + \sqrt{2}$, but we further assert that in $\mathbb{F}_q$, $2 + \sqrt{2}$ has odd order, and thus all 2-power roots exist. This is quick to see because $(2 + \sqrt{2})^{(q-1)/2} = (z^2)^{(q-1)/2} = z^{q-1} = 1$.

We now find $\sqrt{z(2+z)}$, which amounts to finding square roots of z and $2 + z$. By the above, we already have a square root of z, so we just need to show the existence of the square root of $2 + z$. This is simple if we let $w = \zeta_{32} + \zeta_{32}^{-1}$ in $\mathbb{F}_p$, which we know to exist if $q \equiv -1 \pmod{32}$. Then $w^2 = 2 + z$.

It remains to find $\sqrt{\sqrt{2}(z-1)}$. Again it suffices to just find a square root of $z-1$. To show such a root exists, consider

$$(z-1)(-z-1) = -z^2+1 = 1-\sqrt{2} = (-1)(1+\sqrt{2}).$$

Note that $z = \sqrt[4]{2}\sqrt{(1+\sqrt{2})}$, and that $1+\sqrt{2}$ is a square because $\sqrt[4]{2}$ and z are squares, but -1 is not a square modulo q since $q \equiv -1 \pmod 4$, so $(z-1)(-z-1)$ is not a square. This implies that exactly one of $(z-1)$ and $(-z-1)$ is a square. So we choose the appropriate z' such that $z'-1$ is a square and we are done.

Since all adjoined elements exist in $\mathbb{F}_q$, we are good to construct points R such that $4R = 2Q = P$. Similar to Theorem 10, this implies that we can tighten the condition that $|P| \mid 2^{p-1}$ further by $|P| \mid 2^{p-3}$, and so by Corollary 4, p must divide $F_k(E, P)$ for some $k \leq p-4$. □

Acknowledgements

We would like to thank the Wake Forest Department of Mathematics and Statistics for their hospitality and resources. The authors used Magma version 2.22-9 [Bosma et al. 1997] and Sage version 7.5.1 [SageMath 2017] for computations. The authors would like to thank Joe Silverman and Katherine Stange for helpful comments, and we would also like to thank the anonymous referee for helpful comments and references which have substantially improved the paper.

References

[Abatzoglou et al. 2016] A. Abatzoglou, A. Silverberg, A. V. Sutherland, and A. Wong, "A framework for deterministic primality proving using elliptic curves with complex multiplication", *Math. Comp.* **85**:299 (2016), 1461–1483. MR Zbl

[Atkin and Morain 1993] A. O. L. Atkin and F. Morain, "Elliptic curves and primality proving", *Math. Comp.* **61**:203 (1993), 29–68. MR Zbl

[Ayad 1992] M. Ayad, "Points S-entiers des courbes elliptiques", *Manuscripta Math.* **76**:3-4 (1992), 305–324. MR Zbl

[Bosma et al. 1997] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system, I: The user language", *J. Symbolic Comput.* **24**:3-4 (1997), 235–265. MR Zbl

[Bugeaud et al. 2006] Y. Bugeaud, M. Mignotte, and S. Siksek, "Classical and modular approaches to exponential Diophantine equations, I: Fibonacci and Lucas perfect powers", *Ann. of Math.* (2) **163**:3 (2006), 969–1018. MR Zbl

[Cohen 2007] H. Cohen, *Number theory, I: Tools and Diophantine equations*, Graduate Texts in Mathematics **239**, Springer, 2007. MR Zbl

[Denomme and Savin 2008] R. Denomme and G. Savin, "Elliptic curve primality tests for Fermat and related primes", *J. Number Theory* **128**:8 (2008), 2398–2412. MR Zbl

[Dummit and Foote 2004] D. S. Dummit and R. M. Foote, *Abstract algebra*, 3rd ed., John Wiley & Sons, Hoboken, NJ, 2004. MR Zbl

[Everest et al. 2004] G. Everest, V. Miller, and N. Stephens, "Primes generated by elliptic curves", *Proc. Amer. Math. Soc.* **132**:4 (2004), 955–963. MR Zbl

[Everest et al. 2008] G. Everest, P. Ingram, V. Mahé, and S. Stevens, "The uniform primality conjecture for elliptic curves", *Acta Arith.* **134**:2 (2008), 157–181. MR Zbl

[Fermat 1894] P. de Fermat, *Œuvres de Pierre Fermat, II*, edited by P. Tannery and C. Henry, Gauthier-Villars et Fils, Paris, 1894.

[Gross 2005] B. H. Gross, "An elliptic curve test for Mersenne primes", *J. Number Theory* **110**:1 (2005), 114–119. MR Zbl

[Koblitz 1987] N. Koblitz, "Elliptic curve cryptosystems", *Math. Comp.* **48**:177 (1987), 203–209. MR Zbl

[Lenstra 1987a] H. W. Lenstra, Jr., "Elliptic curves and number-theoretic algorithms", pp. 99–120 in *Proceedings of the International Congress of Mathematicians, I* (Berkeley, CA., 1986), edited by A. M. Gleason, Amer. Math. Soc., Providence, RI, 1987. MR Zbl

[Lenstra 1987b] H. W. Lenstra, Jr., "Factoring integers with elliptic curves", *Ann. of Math.* (2) **126**:3 (1987), 649–673. MR Zbl

[Miller 1986] V. S. Miller, "Use of elliptic curves in cryptography", pp. 417–426 in *Advances in cryptology: CRYPTO '85* (Santa Barbara, CA, 1985), edited by H. C. Williams, Lecture Notes in Comput. Sci. **218**, Springer, 1986. MR Zbl

[Poonen et al. 2007] B. Poonen, E. F. Schaefer, and M. Stoll, "Twists of $X(7)$ and primitive solutions to $x^2 + y^3 = z^7$", *Duke Math. J.* **137**:1 (2007), 103–158. MR Zbl

[SageMath 2017] The Sage Developers, *SageMath, the Sage Mathematics Software System*, 2017, available at http://www.sagemath.org. Version 7.5.1.

[Silverman 1986] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer, 1986. MR Zbl

[Silverman 1994] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer, 1994. MR Zbl

[Silverman and Tate 1992] J. H. Silverman and J. Tate, *Rational points on elliptic curves*, Springer, 1992. MR Zbl

[Thue 1909] A. Thue, "Über Annäherungswerte algebraischer Zahlen", *J. Reine Angew. Math.* **135** (1909), 284–305. MR Zbl

[Tsumura 2011] Y. Tsumura, "Primality tests for $2^p \pm 2^{(p+1)/2} + 1$ using elliptic curves", *Proc. Amer. Math. Soc.* **139**:8 (2011), 2697–2703. MR Zbl

[Tzanakis and de Weger 1989] N. Tzanakis and B. M. M. de Weger, "On the practical solution of the Thue equation", *J. Number Theory* **31**:2 (1989), 99–132. MR Zbl

[Wiles 1995] A. Wiles, "Modular elliptic curves and Fermat's last theorem", *Ann. of Math.* (2) **141**:3 (1995), 443–551. MR Zbl

Received: 2017-08-12 Revised: 2018-07-17 Accepted: 2018-07-22

skye@gatech.edu
Department of Mathematics, Reed College, Portland, OR, United States

randydominick1093@gmail.com
Department of Mathematics & Statistics,
Texas Tech University, Lubbock, TX, United States

mk6673@bard.edu
Department of Mathematics, Bard College,
Annandale-on-Hudson, NY, United States

rouseja@wfu.edu
Department of Mathematics and Statistics,
Wake Forest University, Winston-Salem, NC, United States

alexandra_walsh@brown.edu
Mathematics Department, Brown University, Providence, RI, United States

involve

msp.org/involve

INVOLVE YOUR STUDENTS IN RESEARCH

Involve showcases and encourages high-quality mathematical research involving students from all academic levels. The editorial board consists of mathematical scientists committed to nurturing student participation in research. Bridging the gap between the extremes of purely undergraduate research journals and mainstream research journals, *Involve* provides a venue to mathematicians wishing to encourage the creative involvement of students.

Cover: Alex Scorpan

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2019 is US $195/year for the electronic version, and $260/year (+$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFlow® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

involve

2019 vol. 12 no. 3