DETERMINISTIC ELLIPTIC CURVE PRIMALITY PROVING FOR A SPECIAL SEQUENCE OF NUMBERS

ALEXANDER ABATZOGLOU, ALICE SILVERBERG,
ANDREW V. SUTHERLAND, AND ANGELA WONG

Abstract. We give a deterministic algorithm that very quickly proves the primality or compositeness of the integers N in a certain sequence, using an elliptic curve $E/\mathbb{Q}$ with complex multiplication by the ring of integers of $\mathbb{Q}(\sqrt{-7})$. The algorithm uses $O(\log N)$ arithmetic operations in the ring $\mathbb{Z}/N\mathbb{Z}$, implying a bit complexity that is quasi-quadratic in $\log N$. Notably, neither of the classical "$N-1$" or "$N+1$" primality tests apply to the integers in our sequence. We discuss how this algorithm may be applied, in combination with sieving techniques, to efficiently search for very large primes. This has allowed us to prove the primality of several integers with more than 100,000 decimal digits, the largest of which has more than a million bits in its binary representation. We believe that this is the largest proven prime N for which no significant partial factorization of $N-1$ or $N+1$ is known.

1. Introduction

With the celebrated result of Agarwal, Kayal, and Saxena [1], one can now unequivocally determine the primality or compositeness of any integer in deterministic polynomial time. With the improvements of Lenstra and Pomerance [21], the AKS algorithm runs in $\tilde{O}(n^6)$ time, where n is the size of the integer to be tested (in bits). However, it has long been known that for certain special sequences of integers, one can do much better. The two most famous examples are the Fermat numbers $F_k = 2^{2^k} + 1$, to which one may apply Pépin's criterion [28], and the Mersenne numbers $M_p = 2^p - 1$, which are subject to the Lucas-Lehmer test [18]. In both cases, the corresponding algorithms are deterministic and run in $\tilde{O}(n^2)$ time.

In fact, every prime admits a proof of its primality that can be verified by a deterministic algorithm in $\tilde{O}(n^2)$ time. Pomerance shows in [29] that for every prime $p > 31$ there exists an elliptic curve $E/\mathbb{F}_p$ with an $\mathbb{F}_p$-rational point P of order $2^r > (p^{1/4}+1)^2$, which allows one to establish the primality of p using just r elliptic curve group operations. Elliptic curves play a key role in Pomerance's proof; the best analogous result using classical primality certificates yields an $\tilde{O}(n^3)$ time bound [31], cf. [6, Thm. 4.1.9].

The difficulty in applying Pomerance's result lies in finding the pair (E, P), a task for which no efficient method is currently known. Rather than searching for suitable pairs (E, P), we instead fix a finite set of curves $E_a/\mathbb{Q}$, each equipped with a known rational point P_a of infinite order. To each positive integer k we associate one of the curves E_a and define an integer J_k for which we give a necessary and sufficient condition for primality: J_k is prime if and only if the reduction of P_a

This work was supported by the National Science Foundation under grants CNS-0831004 and DMS-1115455.

in $E_a(\mathbb{F}_p)$ has order 2^{k+1} for every prime p dividing J_k. Of course $p = J_k$ when J_k is prime, but this condition can easily be checked without knowing the prime factorization of J_k. This yields a deterministic algorithm that runs in $\tilde{O}(n^2)$ time (see Algorithm 5.1).

Our results extend the methods used by Gross [14], Denomme and Savin [7], Tsumura [37], and Gurevich and Kunyavskiĭ [16], all of which fit within a general framework laid out by Chudnovsky and Chudnovsky in [5] for determining the primality of integers in special sequences using elliptic curves with complex multiplication (CM). The elliptic curves that we use lie in the family of quadratic twists defined by the equations

$$E_a : y^2 = x^3 - 35a^2x - 98a^3, \tag{1}$$

for square-free integers a such that $E_a(\mathbb{Q})$ has positive rank. Each curve has good reduction outside of 2, 7, and the prime divisors of a, and has CM by $\mathbb{Z}[\alpha]$, where

$$\alpha = \frac{1+\sqrt{-7}}{2}.$$

For each curve E_a, we fix a point $P_a \in E_a(\mathbb{Q})$ of infinite order with $P_a \notin 2E_a(\mathbb{Q})$.

For each positive integer k, let

$$j_k = 1 + 2\alpha^k \in \mathbb{Z}[\alpha], \qquad J_k = j_k\bar{j}_k = 1 + 2(\alpha^k + \bar{\alpha}^k) + 2^{k+2} \in \mathbb{N}.$$

The integer sequence J_k satisfies the linear recurrence relation

$$J_{k+4} = 4J_{k+3} - 7J_{k+2} + 8J_{k+1} - 4J_k,$$

with initial values $J_1 = J_2 = 11$, $J_3 = 23$, and $J_4 = 67$. Then (by Lemma 4.5) J_k is composite for $k \equiv 0 \pmod 8$ and for $k \equiv 6 \pmod{24}$. To each other value of k we assign a squarefree integer a, based on the congruence class of $k \pmod{72}$, as listed in Table 1. Our choice of a is based on two criteria. First, it ensures that when J_k is prime, the Frobenius endomorphism of E_a mod J_k corresponds to complex multiplication by j_k (rather than $-j_k$) and

$$E_a(\mathbb{Z}/J_k\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k+1}\mathbb{Z}.$$

Second, it implies that when J_k is prime, the reduction of the point P_a has order 2^{k+1} in $E(\mathbb{Z}/J_k\mathbb{Z})$. The second condition is actually stronger than necessary (in general, one only needs P_a to have order greater than $2^{k/2+1}$), but it simplifies matters. Note that choosing a sequence of the form $j_k = 1 + \Lambda_k$ means that $E_a(\mathbb{Z}[\alpha]/(j_k)) \simeq \mathbb{Z}[\alpha]/\Lambda_k$, whenever J_k is prime and j_k is the Frobenius endomorphism of E_a mod J_k (see Lemma 4.6).

We prove in Theorem 4.1 that the integer J_k is prime if and only if the point P_a has order 2^{k+1} on "E_a mod J_k". More precisely, we prove that if one applies the standard formulas for the elliptic curve group law to compute scalar multiples $Q_i = 2^iP_a$ using projective coordinates $Q_i = [x_i, y_i, z_i]$ in the ring $\mathbb{Z}/J_k\mathbb{Z}$, then J_k is prime if and only if $\gcd(J_k, z_k) = 1$ and $z_{k+1} = 0$. This allows us to determine whether J_k is prime or composite using $O(k)$ operations in the ring $\mathbb{Z}/J_k\mathbb{Z}$, yielding a bit complexity of $O(k^2 \log k \log\log k) = \tilde{O}(k^2)$ (see Proposition 5.2 for a more precise bound).

We note that, unlike the Fermat numbers, the Mersenne numbers, and many similar numbers of a special form, the integers J_k are not amenable to any of the classical "$N - 1$" or "$N + 1$" type primality tests (or combined tests) that are typically used to find very large primes (indeed, the 1000 largest primes currently listed in [4] all have the shape $ab^n \pm 1$ for some small integers a and b).

In combination with a sieving approach described in §5, we have used our algorithm to determine the primality of J_k for all $k \leq 10^6$. The prime values of J_k are listed in Table 4. We have also proven that J_k is prime for $k = 1{,}111{,}930$, which we believe is the largest proven prime N for which no significant partial factorization of either $N - 1$ or $N + 1$ is known.

Generalizations have been suggested to the settings of higher dimensional abelian varieties with complex multiplication, algebraic tori, and group schemes by Chudnovsky and Chudnovsky [5], Gross [14], and Gurevich and Kunyavskiĭ [15], respectively. In the PhD theses of the first and fourth authors, and in a forthcoming paper, we are extending the results in this paper to a more general framework.

Acknowledgments: We thank Daniel J. Bernstein, François Morain, Carl Pomerance, and Karl Rubin for helpful conversations, and the organizers of ECC 2010, the First Abel Conference, and the AWM Anniversary Conference where useful discussions took place. We thank the reviewers for helpful comments.

2. Relation to Prior Work

In [5], Chudnovsky and Chudnovsky consider certain sequences of integers $s_k = \mathrm{Norm}_{K/\mathbb{Q}}(1 + \alpha_0\alpha_1^k)$, defined by algebraic integers α_0 and α_1 in an imaginary quadratic field $K = \mathbb{Q}(\sqrt{D})$. They give sufficient conditions for the primality of s_k, using an elliptic curve E with CM by K. In our setting, $D = -7$, $\alpha_0 = 2$, $\alpha_1 = (1 + \sqrt{-7})/2$, and $J_k = s_k$. The key difference here is that we give necessary and sufficient criteria for primality that can be efficiently checked by a deterministic algorithm. This is achieved by carefully selecting the curves $E_a/\mathbb{Q}$ that we use, so that in each case we are able to prove that the point $P_a \in E_a(\mathbb{Q})$ reduces to a point of maximal order 2^{k+1} on E_a mod J_k, whenever J_k is prime. Without such a construction, we know of no way to obtain *any* non-trivial point on E mod s_k in deterministic polynomial time.

Our work is a direct extension of the techniques developed by Gross [14, 38], Denomme and Savin [7], Tsumura [37], and Gurevich and Kunyavskiĭ [16], who use elliptic curves with CM by the ring of integers of $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$ to test the primality of Mersenne, Fermat, and related numbers. However, as noted by Pomerance [30, §4], the integers considered in [7] can be proved prime using classical methods that are more efficient and do not involve elliptic curves, and the same applies to [14, 37, 38, 16]. But this is not the case for the sequence we consider here.

3. Background and Notation

3.1. **Elliptic curve primality proving.** Primality proving algorithms based on elliptic curves have been proposed since the mid-1980s. Bosma [3] and Chudnovsky and Chudnovsky [5] considered a setting similar to the one employed here, using elliptic curves to prove the primality of numbers of a special form; Bosma proposed the use of elliptic curves with complex multiplication by $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$, while Chudnovsky and Chudnovsky considered a wider range of elliptic curves and other algebraic varieties. Goldwasser and Kilian [11, 12] gave the first general purpose elliptic curve primality proving algorithm, using randomly generated elliptic curves.

Atkin and Morain [2, 26] developed an improved version of the Goldwasser-Kilian algorithm that uses the CM method to construct the elliptic curves used, rather than generating them at random (it does rely on probabilistic methods for root-finding). With asymptotic improvements due to Shallit, the Atkin-Morain algorithm has a heuristic expected running time of $\tilde{O}(n^4)$, which makes it the method of choice for general purpose primality proving [27]. Gordon [13] proposed a general purpose compositeness test using supersingular reductions of CM elliptic curves over $\mathbb{Q}$.

Throughout this paper, if $E \subset \mathbb{P}^2$ is an elliptic curve over $\mathbb{Q}$, we shall write points $[x, y, z] \in E(\mathbb{Q})$ so that $x, y, z \in \mathbb{Z}$ and $\gcd(x, y, z) = 1$, and we may use (x, y) to denote the projective point $[x, y, 1]$.

We say that a point $P = [x, y, z] \in E(\mathbb{Q})$ is *zero mod N* when N divides z; otherwise P is *nonzero mod N*. Note that if P is zero mod N then P is zero mod p for all primes p dividing N.

Definition 3.1. *Given an elliptic curve E over $\mathbb{Q}$, a point $P = [x, y, z] \in E(\mathbb{Q})$, and $N \in \mathbb{Z}$, we say that P is* strongly nonzero mod N if $\gcd(z, N) = 1$.

If P is strongly nonzero mod N, then P is nonzero mod p for every prime $p|N$, and if N is prime, then P is strongly nonzero mod N if and only if P is nonzero mod N.

We rely on the following fundamental result, which can be found in [11, 20, 12].

Proposition 3.2. *Let $E/\mathbb{Q}$ be an elliptic curve, let N be a positive integer prime to* $\operatorname{disc}(E)$*, let $P \in E(\mathbb{Q})$, and let $m > (N^{1/4} + 1)^2$. Suppose mP is zero mod N and $(m/q)P$ is strongly nonzero mod N for all primes $q|m$. Then N is prime.*

To make practical use of Proposition 3.2, one needs to know the prime factorization of m. For general elliptic curve primality proving this presents a challenge; the algorithms of Goldwasser-Kilian and Atkin-Morain use different approaches to ensure that m has an easy factorization, but both must then recursively construct primality proofs for the primes q dividing m. In our restricted setting we effectively fix the prime factorization of $m = 2^{k+1}$ ahead of time.

Next we give a variant of Proposition 3.2 that replaces "strongly nonzero" with "nonzero", at the expense of m being a prime power with a larger lower bound.

Proposition 3.3. *Let $E/\mathbb{Q}$ be an elliptic curve, let p be a prime, let N be an odd positive integer prime to $p\operatorname{disc}(E)$, and let $P \in E(\mathbb{Q})$. Suppose b is a positive integer such that $p^b > (\sqrt{N/3} + 1)^2$ and $p^b P$ is zero mod N and $p^{b-1}P$ is nonzero mod N. Then N is prime.*

Proof. Since $p^{b-1}P$ is nonzero mod N, there are a prime divisor q of N and a positive integer r such that q^r exactly divides N and $p^{b-1}P$ is nonzero mod q^r. Let $E_1(\mathbb{Z}/q^r\mathbb{Z})$ denote the kernel of the reduction map $E(\mathbb{Z}/q^r\mathbb{Z}) \to E(\mathbb{F}_q)$. It follows, for example, from [23, Thm. 4.1] that $E_1(\mathbb{Z}/q^r\mathbb{Z})$ is a q-group. Let $P' \in E(\mathbb{Z}/q^r\mathbb{Z})$ be the reduction of P mod q^r and let P'' be the image of P' in $E(\mathbb{F}_q)$. If $p^{b-1}P'' = 0$ then $p^{b-1}P' \in E_1(\mathbb{Z}/q^r\mathbb{Z})$, so $p^{b-1}P'$ has order a power of q. But by assumption it has order p, which is prime to N. This is a contradiction, so P'' has order p^b. If N were composite, then $q \leq N/3$ since N is odd, so by the Hasse bound,

$$p^b \leq |E(\mathbb{F}_q)| \leq (\sqrt{q} + 1)^2 \leq (\sqrt{N/3} + 1)^2,$$

contradicting the hypothesis that $p^b > (\sqrt{N/3} + 1)^2$. □

3.2. **Complex multiplication and Frobenius endomorphism.** For any number field F, let $\mathcal{O}_F$ denote its ring of integers. If E is an elliptic curve over a field K, and Ω_K is the space of holomorphic differentials on E over K, then Ω_K is a one-dimensional K-vector space, and there is a canonical ring homomorphism

$$\mathrm{End}_K(E) \to \mathrm{End}_K(\Omega) = K. \tag{2}$$

Suppose now that E is an elliptic curve over an imaginary quadratic field K, and that E has complex multiplication (CM) by $\mathcal{O}_K$, meaning that $\mathrm{End}_K(E) \simeq \mathcal{O}_K$. Then the image of the map in (2) is $\mathcal{O}_K$. Let $\psi : \mathcal{O}_K \to \mathrm{End}_K(E)$ denote the inverse map. Suppose that $\mathfrak{p}$ is a prime ideal of K at which E has good reduction and let $\tilde{E}$ denote the reduction of E mod $\mathfrak{p}$. Then the composition

$$\mathcal{O}_K \xrightarrow{\sim} \mathrm{End}_K(E) \hookrightarrow \mathrm{End}_{\mathcal{O}_K/\mathfrak{p}}(\tilde{E}),$$

where the first map is ψ and the second is induced by reduction mod $\mathfrak{p}$, gives a canonical embedding

$$\mathcal{O}_K \hookrightarrow \mathrm{End}(\tilde{E}). \tag{3}$$

The Frobenius endomorphism of $\tilde{E}$ is $(x, y) \mapsto (x^q, y^q)$ where $q = \mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{p})$; under the embedding in (3), the Frobenius endomorphism is the image of a particular generator π of the (principal) ideal $\mathfrak{p}$. By abuse of notation, we say that the Frobenius endomorphism is π.

4. Main Theorem

In this section we state and prove our main result, Theorem 4.1, which gives a necessary and sufficient condition for the primality of the numbers J_k.

Fix a particular square root of -7 and let $K = \mathbb{Q}(\sqrt{-7})$. Let

$$\alpha = \frac{1 + \sqrt{-7}}{2} \in \mathcal{O}_K,$$

and for each positive integer k, let

$$j_k = 1 + 2\alpha^k \in \mathbb{Z}[\alpha] \qquad \text{and} \qquad J_k = \mathrm{Norm}_{K/\mathbb{Q}}(j_k) = j_k \bar{j}_k \in \mathbb{N}.$$

Note that J_k is prime in $\mathbb{Z}$ if and only if j_k is prime in $\mathcal{O}_K$. Note also that $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = \alpha\bar{\alpha} = 2$.

Recall the family of elliptic curves E_a defined by (1). Lemma 4.5 below shows that J_k is composite if $k \equiv 0 \pmod 8$ or $k \equiv 6 \pmod{24}$, so we omit these cases from our primality criterion. For each remaining value of k, Table 1 lists the twisting parameter a and the point $P_a \in E_a(\mathbb{Q})$ we associate to k. For each of these a, the elliptic curve E_a has rank one over $\mathbb{Q}$, and the point P_a is a generator for $E_a(\mathbb{Q})$ modulo torsion.

Table 1. The twisting parameters a and points P_a

k	a	P_a
$k \equiv 0$ or $2 \pmod 3$	-1	$(1, 8)$
$k \equiv 4, 7, 13, 22 \pmod{24}$	-5	$(15, 50)$
$k \equiv 10 \pmod{24}$	-6	$(21, 63)$
$k \equiv 1, 19, 49, 67 \pmod{72}$	-17	$(81, 440)$
$k \equiv 25, 43 \pmod{72}$	-111	$(-633, 12384)$

Theorem 4.1. *Fix $k > 1$ such that $k \not\equiv 0 \pmod 8$ and $k \not\equiv 6 \pmod{24}$. Let $P_a \in E_a(\mathbb{Q})$ be as in Table 1 (depending on k). The following are equivalent:*

(i) *$2^{k+1}P_a$ is zero mod J_k and $2^k P_a$ is strongly nonzero mod J_k;*
(ii) *J_k is prime.*

Remark 4.2. Applying Proposition 3.3 with $N = J_k$, $p = 2$, and $b = k + 1$, we can add an equivalent condition in Theorem 4.1 as long as $k \geq 6$, namely:

(iii) $2^{k+1}P_a$ is zero mod J_k and $2^k P_a$ is nonzero mod J_k.

We shall prove Theorem 4.1 via a series of lemmas, but let us first outline the proof. One direction is easy: since $2^{k+1} > (J_k^{1/4} + 1)^2$ for all $k > 1$, if (i) holds then so does (ii), by Proposition 3.2.

Now fix a and P_a as in Table 1, and let $\tilde{P}_a$ denote the reduction of P_a modulo j_k. We first compute a set S_a such that if $k \in S_a$ and j_k is prime, then $E_a(\mathcal{O}_K/(j_k)) \simeq \mathcal{O}_K/(2\alpha^k)$ as $\mathcal{O}_K$-modules. We then compute a set T_a such that if $k \in T_a$ and j_k is prime, then $\tilde{P}_a$ does not lie in $\alpha E_a(\mathcal{O}_K/(j_k))$ if and only if $k \in T_a$ (note that $\alpha \in \mathcal{O}_K \hookrightarrow \mathrm{End}(E_a)$). For $k \in S_a \cap T_a$, the point $\tilde{P}_a$ has order 2^{k+1} whenever J_k is prime, and we can use Proposition 3.2 to prove that J_k is prime.

We now fill in the details. Many of the explicit calculations below were performed with the assistance of the Sage computer algebra system [36].

4.1. **The linear recurrence sequence J_k.** As noted in the introduction, the sequence J_k satisfies the linear recurrence relation

$$J_{k+4} = 4J_{k+3} - 7J_{k+2} + 8J_{k+1} - 4J_k. \tag{4}$$

We now prove this, and also note some periodic properties of this sequence. See [8] or [22, Ch. 6] for basic properties of linear recurrence sequences.

Definition 4.3. *We call a sequence a_k (purely)* periodic *if there exists an integer m such that $a_k = a_{k+m}$ for all k. The minimal such m is the* period *of the sequence.*

Lemma 4.4. *The sequence J_k satisfies (4). If p is an odd prime and $\mathfrak{p} \subset \mathcal{O}_K$ is a prime ideal above (p), then the sequence $J_k \bmod p$ is periodic, with period equal to the least common multiple of the orders of 2 and α in $(\mathcal{O}_K/\mathfrak{p})^*$.*

Proof. The characteristic polynomial of the linear recurrence in (4) is

$$f(x) = x^4 - 4x^3 + 7x^2 - 8x + 4 = (x-1)(x-2)(x^2 - x + 2),$$

whose roots are $1, 2, \alpha$, and $\bar{\alpha}$. It follows that the sequences 1^k, 2^k, α^k, and $\bar{\alpha}^k$, and any linear combination of these sequences, satisfy (4). Thus J_k satisfies (4).

One easily checks that the lemma is true for $p = 7$, so assume $p \neq 7$. Let A be the 4×4 matrix with $A_{i,j} = J_{i+j-1}$. Then $\det A = -2^{12} \cdot 7$ is nonzero mod p, hence its rows are linearly independent over $\mathbb{F}_p$. It follows from Theorems 6.19 and 6.27 of [22] that the sequence $J_k \bmod p$ is periodic, with period equal to the lcm of the orders of the roots of f in $\bar{\mathbb{F}}_p^*$ (which we note are distinct). These roots all lie in $\mathcal{O}_K/\mathfrak{p} \simeq \mathbb{F}_{p^d}$, where $d \in \{1, 2\}$ is the residue degree of $\mathfrak{p}$. Since $\bar{\alpha} = 2/\alpha$, the order of $\bar{\alpha}$ in $(\mathcal{O}_K/\mathfrak{p})^*$ divides the lcm of the orders of 2 and α. The lemma follows. □

When p is an odd prime, let m_p denote the period of the sequence $J_k \bmod p$. Lemma 4.4 implies that m_p always divides $p^2 - 1$, and it divides $p - 1$ whenever p splits in K.

Lemma 4.5. *The following hold:*

(i) *J_k is divisible by* 3 *if and only if* $k \equiv 0 \pmod 8$*;*
(ii) *J_k is divisible by* 5 *if and only if* $k \equiv 6 \pmod{24}$*.*

Proof. Lemma 4.4 allows us to compute the periods $m_3 = 8$ and $m_5 = 24$. It then suffices to check, for $p = 3, 5$, when $J_k \equiv 0 \pmod p$ for $1 \le k \le m_p$.

Alternatively, note that α and $\bar{\alpha}$ each has order 8 in $(\mathcal{O}_K/(3))^\times$. Hence if $k \equiv 0 \pmod 8$, then $J_k = 1+2(\alpha^k+\bar{\alpha}^k)+2^{k+2} \equiv 1+2(1+1)+1 \equiv 0 \pmod 3$. Similarly, $\alpha^6 \equiv 2 \equiv \bar{\alpha}^6 \pmod 5$, so $J_k \equiv 1+2(4)+1 \equiv 0 \pmod 5$. □

4.2. The set S_a.

For each squarefree integer a we define the set of integers

$$S_a := \left\{ k > 1 : \left(\frac{a}{J_k}\right)\left(\frac{j_k}{\sqrt{-7}}\right) = 1 \right\},$$

where $\left(\frac{\ }{\ }\right)$ denotes the (generalized) Jacobi symbol.

If j_k is prime in $\mathcal{O}_K$, then the Frobenius endomorphism of E_a over the finite field $\mathcal{O}_K/(j_k)$ corresponds to either j_k or $-j_k$. For elliptic curves over $\mathbb{Q}$ with complex multiplication, one can easily determine which is the case.

Lemma 4.6. *Suppose a is a squarefree integer, $k > 1$, and j_k is prime in $\mathcal{O}_K$. Then:*

(i) *$k \in S_a$ if and only if the Frobenius endomorphism of E_a over the finite field $\mathcal{O}_K/(j_k)$ is j_k;*
(ii) *if $k \in S_a$, then $E_a(\mathcal{O}_K/(j_k)) \simeq \mathcal{O}_K/(2\alpha^k)$ as $\mathcal{O}_K$-modules.*

Proof. The elliptic curve E_a is the curve in Theorem 1 of [35, p. 1117], with $D = -7$ and $\pi = j_k$. By [35, p. 1135], the Frobenius endomorphism of E_a over $\mathcal{O}_K/(j_k)$ is

$$\left(\frac{a}{J_k}\right)\left(\frac{j_k}{\sqrt{-7}}\right) j_k \in \mathcal{O}_K.$$

Part (i) then follows from the definition of S_a. For (ii), note that (i) implies that if $k \in S_a$, then

$$E_a(\mathcal{O}_K/(j_k)) \simeq \ker(j_k - 1) = \ker(2\alpha^k) \simeq \mathcal{O}_K/(2\alpha^k),$$

which completes the proof. □

Lemma 4.7. *If $k > 1$, then*

(i) $\left(\frac{-1}{J_k}\right) = -1$,
(ii) $\left(\frac{2}{J_k}\right) = \begin{cases} 1 & \text{if } k \text{ is odd,} \\ -1 & \text{if } k \text{ is even.} \end{cases}$

Proof. For $k > 1$, $J_k \equiv 3 \pmod 8$ if k is even, and $J_k \equiv 7 \pmod 8$ if k is odd. □

We now explicitly compute the sets S_a for the values of a used in Theorem 4.1.

Lemma 4.8. *For $a \in \{-1, -5, -6, -17, -111\}$ the sets S_a are as in Table 2.*

Proof. Since $j_k = 1 + 2\alpha^k$, and $\alpha \equiv 4 \pmod{\sqrt{-7}}$, and $2^3 \equiv 1 \pmod 7$, we have

$$\left(\frac{j_k}{\sqrt{-7}}\right) = \left(\frac{1+2^{2k+1}}{7}\right) = \begin{cases} 1 & \text{if } k \equiv 1 \pmod 3, \\ -1 & \text{if } k \equiv 0, 2 \pmod 3. \end{cases}$$

We now need to compute $(\frac{a}{J_k})$ for $a = -1, -5, -6, -17$, and -111. By Lemma 4.7(i), we have $(\frac{-1}{J_k}) = -1$. Applying Lemma 4.4 to the odd primes $p = 3, 5, 17, 37$ that

TABLE 2. The sets S_a

a	m	$S_a = \{k > 1 : k \bmod m \text{ is as below}\}$
-1	3	$0, 2$
-5	24	$0, 2, 4, 5, 7, 9, 12, 13, 16, 18, 21, 22, 23$
-6	24	$3, 7, 9, 10, 11, 12, 13, 17, 20, 22$
-17	144	$0, 1, 5, 7, 9, 10, 13, 14, 15, 18, 19, 20, 22, 23, 27, 30, 31, 33, 34, 36, 42, 43, 44, 45, 49, 50, 53, 56, 61, 62, 63, 66, 67, 68, 70, 71, 72, 73, 75, 76, 78, 79, 80, 81, 82, 83, 90, 91, 92, 93, 97, 99, 100, 104, 106, 108, 110, 111, 112, 114, 117, 118, 121, 122, 123, 125, 126, 128, 129, 133, 135, 136, 137, 138, 139, 141, 143$
-111	72	$2, 4, 6, 9, 14, 15, 18, 20, 22, 23, 25, 30, 33, 34, 35, 37, 38, 39, 41, 42, 43, 47, 49, 50, 52, 53, 54, 55, 57, 58, 63, 65, 66, 67, 68, 70$

can divide a, we find that the periods m_p of the sequences $J_k \bmod p$ are $m_3 = 8$, $m_5 = 24$, $m_{17} = 144$, and $m_{37} = 36$. Since $(\frac{-1}{J_k}) = -1$, it follows from quadratic reciprocity that for $a = -5, -17$, and -111, the period of the sequence $(\frac{a}{J_k})$ divides the least common multiple of the periods m_p for $p|a$. For $a = -6$, by Lemma 4.7(ii) the period of $(\frac{2}{J_k})$ is 2, which already divides $m_3 = 8$. Since 3 is the period of the sequence $(\frac{j_k}{\sqrt{-7}})$, we find the period m of $(\frac{a}{J_k})(\frac{j_k}{\sqrt{-7}})$ listed in Table 2 by taking the least common multiple of 3 and the m_p for $p|a$. To compute S_a, it then suffices to compute $(\frac{a}{J_k})$ and check when $(\frac{a}{J_k}) = (\frac{j_k}{\sqrt{-7}})$, for $1 < k \le m+1$. □

4.3. **The set T_a.** We now define the sets T_a.

Definition 4.9. *Let a be a squarefree integer, and suppose that $P \in E_a(K)$. Then the field $K(\alpha^{-1}(P))$ has degree 1 or 2 over K, so it can be written in the form $K(\sqrt{\delta_P})$ with $\delta_P \in K$. Let*

$$T_P := \left\{k > 1 : \left(\frac{\delta_P}{j_k}\right) = -1\right\}.$$

For the values of a listed in Table 1, let $T_a = T_{P_a}$ and let $\delta_a = \delta_{P_a}$.

Lemma 4.10. *Suppose that $k > 1$, j_k is prime in $\mathcal{O}_K$, and a is a squarefree integer. Suppose that $P \in E_a(K)$, and let $\tilde{P}$ denote the reduction of P mod j_k. Then $\tilde{P} \notin \alpha E_a(\mathcal{O}_K/(j_k))$ if and only if $k \in T_P$.*

Proof. Let $L = K(\alpha^{-1}(P)) = K(\gamma)$ for some $\gamma \in L$ such that $\gamma^2 = \delta_P$. Fix a $Q \in E_a(\bar{\mathbb{Q}})$ such that $\alpha Q = P$. Since $\ker(\alpha) \subset E_a[2] \subset E_a(K)$, we have $K(Q) = L = K(\gamma)$. Fix a prime ideal $\mathfrak{p}$ of L above (j_k), let $\mathbb{F} = \mathcal{O}_K/(j_k)$, let $\tilde{Q} \in E_a(\bar{\mathbb{F}})$ be the reduction of Q mod $\mathfrak{p}$, and let $\tilde{\gamma}$ be the reduction of γ mod $\mathfrak{p}$. Then $\mathbb{F}(\tilde{Q}) = \mathbb{F}(\tilde{\gamma})$.

Now $\tilde{P} \in \alpha E_a(\mathbb{F})$ if and only if $\tilde{Q} \in E_a(\mathbb{F})$. By the above, this happens if and only if $\tilde{\gamma} \in \mathbb{F}$, that is, if and only if δ_P is a square modulo j_k. □

Lemma 4.11. *We can take*

$$\delta_{-1} = \alpha, \quad \delta_{-5} = -5\alpha, \quad \delta_{-6} = -3\sqrt{-7}, \quad \delta_{-17} = \alpha, \quad \delta_{-111} = -3.$$

Proof. The action of the endomorphism α on the elliptic curve E_a and its reductions is as follows (see Proposition II.2.3.1 of [34, p. 111]). For $(x, y) \in E_a$, we have

$$\alpha(x,y) = \left(\frac{2x^2 + a(7-\sqrt{-7})x + a^2(-7-21\sqrt{-7})}{(-3+\sqrt{-7})x + a(-7+5\sqrt{-7})}, \frac{y\left(2x^2 + a(14-2\sqrt{-7})x + a^2(28+14\sqrt{-7})\right)}{-(5+\sqrt{-7})x^2 - a(42+2\sqrt{-7})x - a^2(77-7\sqrt{-7})} \right).$$

Solving for R in $\alpha R = P_a$ yields δ_a in each case. □

Lemma 4.12. *If $k > 1$ then* $\left(\frac{\alpha}{j_k}\right) = -1$.

Proof. Let $M = K(\sqrt{\alpha})$. By the reciprocity law of global class field theory we have

$$\prod_{\mathfrak{p}} (j_k, M_{\mathfrak{p}}/K_{\mathfrak{p}}) = 1,$$

where $(j_k, M_{\mathfrak{p}}/K_{\mathfrak{p}})$ is the norm residue symbol.

Let $f(x) = x^2 - j_k \in \mathcal{O}_{K_\alpha}[x]$. For $k > 1$ we have

$$|f(1)|_\alpha = \left|2\alpha^k\right|_\alpha = 2^{-(k+1)} < 2^{-2} = |4|_\alpha = \left|f'(1)^2\right|_\alpha,$$

and Hensel's lemma implies that $f(x)$ has a root in $\mathcal{O}_{K_\alpha}$. Thus j_k is a square in K_α and $(j_k, M_\alpha/K_\alpha) = 1$.

Identify $K_{\bar\alpha}$ with $\mathbb{Q}_2$. Applying Theorem 1 of [33, p. 20] with $a = j_k$ and $b = \alpha$, and using $\bar\alpha^5 = 5 + \alpha$, gives $(j_k, \alpha) = -1$, where (j_k, α) is the Hilbert symbol. Thus $j_k \notin \operatorname{Norm}_{M_{\bar\alpha}/K_{\bar\alpha}}(M^*_{\bar\alpha})$, and therefore $(j_k, M_{\bar\alpha}/K_{\bar\alpha}) = -1$.

If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ that does not divide 2, then $M_{\mathfrak{p}}/K_{\mathfrak{p}}$ is unramified. By local class field theory we then have

$$(j_k, M_{\mathfrak{p}}/K_{\mathfrak{p}}) = \left(\frac{\alpha}{\mathfrak{p}}\right)^{\operatorname{ord}_{\mathfrak{p}}(j_k)}.$$

Since j_k is prime to 2, we have $\operatorname{ord}_\alpha(j_k) = \operatorname{ord}_{\bar\alpha}(j_k) = 0$, hence

$$\prod_{\mathfrak{p}\nmid 2} (j_k, M_{\mathfrak{p}}/K_{\mathfrak{p}}) = \prod_{\mathfrak{p}\nmid 2} \left(\frac{\alpha}{\mathfrak{p}}\right)^{\operatorname{ord}_{\mathfrak{p}}(j_k)} = \prod_{\text{all } \mathfrak{p}} \left(\frac{\alpha}{\mathfrak{p}}\right)^{\operatorname{ord}_{\mathfrak{p}}(j_k)} = \left(\frac{\alpha}{j_k}\right).$$

Therefore,

$$1 = \prod_{\mathfrak{p}} (j_k, M_{\mathfrak{p}}/K_{\mathfrak{p}}) = \left(\frac{\alpha}{j_k}\right)(j_k, M_\alpha/K_\alpha)(j_k, M_{\bar\alpha}/K_{\bar\alpha}) = -\left(\frac{\alpha}{j_k}\right),$$

as desired. □

Lemma 4.13. *For $a \in \{-1, -5, -6, -17, -111\}$ the sets T_a are as follows:*

$$\begin{aligned}
T_{-1} &= \{k > 1\},\\
T_{-5} &= \{k > 1 : k \equiv 3, 4, 7, 8, 11, 13, 14, 15, 16, 17, 20, 22 \pmod{24}\},\\
T_{-6} &= \{k > 1 : k \equiv 1, 5, 10, 12, 15, 19, 20, 21, 22, 23 \pmod{24}\},\\
T_{-17} &= \{k > 1\},\\
T_{-111} &= \{k > 1 : k \equiv 1, 2, 3, 6 \pmod{8}\}.
\end{aligned}$$

Proof. We apply Lemma 4.11 and the definition of T_a. Lemma 4.12 implies that $T_{-1} = T_{-17} = \{k > 1\}$. For $a = -6$ we use quadratic reciprocity in quadratic fields (see Theorem 8.15 of [19, p. 257]) to compute $\left(\frac{\sqrt{-7}}{j_k}\right)$. For the remaining cases we compute $\left(\frac{-3}{j_k}\right) = \left(\frac{-3}{J_k}\right)$ and $\left(\frac{-5}{j_k}\right) = \left(\frac{-5}{J_k}\right)$ as in the proof of Lemma 4.8, and apply $\left(\frac{\alpha}{j_k}\right) = -1$ from Lemma 4.12. □

4.4. **Proof of Theorem 4.1.**

Lemma 4.14. *Let a be a squarefree integer. Suppose that $P \in E_a(K)$, $k \in S_a \cap T_P$, and j_k is prime. Let $\tilde{P}$ denote the reduction of P mod j_k. Then the annihilator of $\tilde{P}$ in $\mathcal{O}_K$ is divisible by α^{k+1}.*

Proof. We have $E_a(\mathcal{O}_K/(j_k)) \simeq \mathcal{O}_K/(2\alpha^k) = \mathcal{O}_K/(\overline{\alpha}\alpha^{k+1})$, by Lemma 4.6(ii). It then suffices to show $\tilde{P} \notin \alpha E_a(\mathcal{O}_K/(j_k))$, which follows from Lemma 4.10. □

The congruence conditions for k in Table 1 come from taking $S_a \cap T_a$, excluding the cases handled by Lemma 4.5, and adjusting to give disjoint sets.

We now prove Theorem 4.1. Suppose that $k > 1$, $k \not\equiv 0 \pmod 8$, $k \not\equiv 6 \pmod{24}$, and J_k is prime. Let a and P_a be as listed in Table 1. Then $k \in S_a \cap T_a$. Let $\tilde{P}$ denote the reduction of P_a mod j_k. We have $E_a(\mathcal{O}_K/(j_k)) \simeq \mathcal{O}_K/(2\alpha^k)$ by Lemma 4.6(ii), and therefore the annihilator of $\tilde{P}$ in $\mathcal{O}_K$ divides $2\alpha^k$. By Lemma 4.14, the annihilator of $\tilde{P}$ in $\mathcal{O}_K$ is divisible by α^{k+1}. Since $2\alpha^k$ divides 2^{k+1} but α^{k+1} does not divide 2^k, we must have $2^{k+1}\tilde{P} = 0$ and $2^k\tilde{P} \neq 0$. Therefore $2^{k+1}P_a$ is zero mod J_k and $2^k P_a$ is strongly nonzero mod J_k.

For the converse, we apply Proposition 3.2 with $m = 2^{k+1}$, noting that

$$2^{k+1} > ((3 \cdot 2^{k+1})^{\frac{1}{4}} + 1)^2 > (J_k^{1/4} + 1)^2$$

for all $k > 2$, and for $k = 2$ we have $2^{k+1} = 8 > (11^{1/4} + 1)^2 = (J_k^{1/4} + 1)^2$. This proves Theorem 4.1.

5. Algorithm

A naïve implementation of Theorem 4.1 is entirely straightforward, but here we describe a particularly efficient implementation and analyze its complexity. We then discuss how the algorithm may be used in combination with sieving to search for prime values of J_k, and give some computational results.

5.1. **Implementation.**

There are two features of the primality criterion given by Theorem 4.1 worth noting. First, it is only necessary to perform the operation of adding a point on the elliptic curve to itself (doubling), no general additions are required. Second, testing whether a projective point $P = [x, y, z]$ is zero or strongly nonzero modulo an integer J_k only involves the z-coordinate: P is zero mod J_k if and only if $J_k | z$, and P is strongly nonzero mod J_k if and only if $\gcd(z, J_k) = 1$.

To reduce the cost of doubling, we transform the curve

$$E_a\colon \qquad y^2 = x^3 - 35a^2x - 98a^3$$

to the Montgomery form [25]

$$E_{A,B}\colon \qquad By^2 = x^3 + Ax^2 + x.$$

Such a transformation is not possible over $\mathbb{Q}$, but it can be done over $\mathbb{Q}(\sqrt{-7})$. In general, one transforms a short Weierstrass equation $y^2 = f(x) = x^3 + a_4x + a_6$ into Montgomery form by choosing a root γ of $f(x)$ and setting $B = (3\gamma^2 - a_4)^{-1/2}$ and $A = 3\gamma B$; see, e.g., [17]. For the curve E_a, we choose $\gamma = \frac{1}{2}(-7 + \sqrt{-7})a$, yielding

$$A = \frac{-15 - 3\sqrt{-7}}{8} \qquad \text{and} \qquad B = \frac{7 + 3\sqrt{-7}}{56a}.$$

With this transformation, the point $P_a = (x_0, y_0)$ on E_a corresponds to the point $(B(x_0 - \gamma), By_0)$ on the Montgomery curve $E_{A,B}$, and is defined over $\mathbb{Q}(\sqrt{-7})$.

In order to apply this transformation modulo J_k, we need a square root of -7 in $\mathbb{Z}/J_k\mathbb{Z}$. If J_k is prime and $d = 7^{(J_k+1)/4}$, then

$$d^2 \equiv 7^{(J_k-1)/2} \cdot 7 \equiv \left(\frac{7}{J_k}\right) 7 \equiv -7 \pmod{J_k},$$

since $J_k \equiv 3 \pmod 4$ and $J_k \equiv 2, 4 \pmod 7$ is a quadratic residue modulo 7. If we find that $d^2 \not\equiv -7 \pmod{J_k}$, then we immediately know that J_k must be composite and no further computation is required.

With the transformation to Montgomery form, the formulas for doubling a point on E_a become particularly simple. If $P = [x_1, y_1, z_1]$ is a projective point on $E_{A,B}$ and $2P = [x_2, y_2, z_2]$, we may determine $[x_2, z_2]$ from $[x_1, z_1]$ via

$$\begin{aligned} 4x_1z_1 &= (x_1 + z_1)^2 - (x_1 - z_1)^2, \\ x_2 &= (x_1 + z_1)^2 (x_1 - z_1)^2, \\ z_2 &= 4x_1z_1\big((x_1 - z_1)^2 + C(4x_1z_1)\big), \end{aligned} \tag{5}$$

where

$$C = (A + 2)/4 = \frac{1 - 3\sqrt{-7}}{32}.$$

Note that C does not depend on P (or even a), and may be precomputed. Thus doubling requires just 2 squarings, 3 multiplications, and 4 additions in $\mathbb{Z}/J_k\mathbb{Z}$.

We now present the algorithm, which exploits the transformation of E_a into Montgomery form. We assume that elements of $\mathbb{Z}/J_k\mathbb{Z}$ are uniquely represented as integers in $[0, J_k - 1]$.

Algorithm 5.1
Input: positive integers k and J_k.
Output: `true` if J_k is prime and `false` if J_k is composite.

1. If $k \equiv 0 \pmod 8$ or $k \equiv 6 \pmod{24}$ then return `false`.
2. Compute $d = 7^{(J_k+1)/4} \bmod J_k$.
3. If $d^2 \not\equiv -7 \pmod{J_k}$ then return `false`.
4. Determine a via Table 1, depending on $k \pmod{72}$.
5. Compute $r = (-7 + d)a/2 \bmod J_k$, $B = (7 + 3d)/(56a) \bmod J_k$, and $C = (1 - 3d)/32 \bmod J_k$.
6. Let $x_1 = B(x_0 - r) \bmod J_k$ and $z_1 = 1$, where $P_a = (x_0, y_0)$ is as in Table 1.
7. For i from 1 to $k + 1$, compute $[x_i, z_i]$ from $[x_{i-1}, z_{i-1}]$ via (5).
8. If $\gcd(z_k, J_k) = 1$ and $J_k | z_{k+1}$ then return `true`, otherwise return `false`.

The tests in step 1 rule out cases where J_k is divisible by 3 or 5, by Lemma 4.5; J_k is then composite, since $J_k > 5$ for all k. This also ensures $\gcd(a, J_k) = 1$, so the divisions in step 5 are all valid (J_k is never divisible by 2 or 7). By Remark 4.2, for $k \geq 6$ the condition $\gcd(z_k, J_k) = 1$ in step 8 can be replaced with $z_k \not\equiv 0 \bmod J_k$.

Proposition 5.2. *Algorithm 5.1 performs $6k + o(k)$ multiplications and $4k$ additions in $\mathbb{Z}/J_k\mathbb{Z}$. Its time complexity is $O(k^2 \log k \log\log k)$ and it uses $O(k)$ space.*

Proof. Using standard techniques for fast exponentiation [39], step 2 uses $k + o(k)$ multiplications in $\mathbb{Z}/J_k\mathbb{Z}$. Steps 5-6 perform $O(1)$ operations in $\mathbb{Z}/J_k\mathbb{Z}$ and step 7 uses $5k$ multiplications and $4k$ additions. The cost of the divisions in step 5 are comparatively negligible, as is the cost of step 8. Multiplications (and additions) in $\mathbb{Z}/J_k\mathbb{Z}$ have a bit complexity of $O(\mathsf{M}(k))$, where $\mathsf{M}(k)$ counts the bit operations needed to multiply two k-bit integers [10, Thm. 9.8]. The bound on the time complexity of Algorithm 5.1 then follows from the Schönhage-Strassen [32] bound: $\mathsf{M}(k) = O(k \log k \log\log k)$. The space complexity bound is immediate: the algorithm only needs to keep track of two pairs $[x_i, z_i]$ and $[x_{i-1}, z_{i-1}]$ at any one time, and elements of $\mathbb{Z}/J_k\mathbb{Z}$ can be represented using $O(k)$ bits. □

TABLE 3. Timings for Algorithm 5.1
(CPU seconds on a 3.0 GHz AMD Phenom II 945)

k	step 2	step 7
$2^{10}+1$	0.00	0.01
$2^{11}+1$	0.00	0.02
$2^{12}+1$	0.02	0.15
$2^{13}+1$	0.15	0.91
$2^{14}+1$	0.88	5.50
$2^{15}+1$	5.26	32.2
$2^{16}+1$	27.5	183
$2^{17}+1$	133	983
$2^{18}+1$	723	5010
$2^{19}+1$	3310	23600
$2^{20}+1$	13700	107000

Table 3 gives timings for Algorithm 5.1 when implemented using the `gmp` library for all integer arithmetic, including the gcd computations. We list the times for step 2 and step 7 separately (the time spent on the other steps is negligible). In the typical case, where J_k is composite, the algorithm is very likely[1] to terminate in step 2, which effectively determines whether J_k is a strong probable prime base -7, as in [6, Alg. 3.5.3]. To obtain representative timings at the values of k listed, we temporarily modified the algorithm to skip step 2.

We note that the timings for step 7 are suboptimal due to the fact that we used the `gmp` function `mpz_mod` to perform modular reductions. A lower level implementation (using Montgomery reduction [24], for example) might improve these timings by perhaps 20 or 30 percent.

We remark that Algorithm 5.1 can easily be augmented, at essentially no additional cost, to retain an intermediate point $Q = [x_s, y_s, z_s]$, where $s = k + 1 - r$ is chosen so that the order 2^r of Q is the least power of 2 greater than $(J_k^{1/4}+1)^2$. The value of y_s may be obtained as a square root of $y_s^2 = (x_s^3 + Ax_s^2 z_s + x_s z_s^2)/(Bz_s)$ by computing $(y_s^2)^{(J_k+1)/4}$. When J_k is prime, the algorithm can then output a Pomerance-style certificate $(E_{A,B}, Q, r, J_k)$ for the primality of J_k. This certificate has the virtue that it can be verified using just $2.5k+O(1)$ multiplications in $\mathbb{Z}/J_k\mathbb{Z}$, versus the $6k + o(k)$ multiplications used by Algorithm 5.1, by checking that the point Q has order 2^r on the elliptic curve $E_{A,B}$ mod J_k.

[1] Indeed, we have yet to encounter even a single J_k that is a strong pseudoprime base -7.

TABLE 4. Prime values of $J_k \approx 2^{k+2}$ for $k \le 10^6$.

k	J_k	a	k	J_k	a	k	J_k	a
2	11	-1	319	427...247	-5	17807	110...799	-1
3	23	-1	375	307...023	-1	18445	125...407	-5
4	67	-5	467	152...727	-1	19318	793...763	-5
5	151	-1	489	639...239	-1	26207	495...799	-1
7	487	-5	494	204...963	-1	27140	359...907	-1
9	2039	-1	543	115...143	-1	31324	116...867	-5
10	4211	-6	643	145...399	-17	36397	155...007	-5
17	524087	-1	684	321...531	-1	47294	327...963	-1
18	1046579	-1	725	706...551	-1	53849	583...567	-1
28	107...427	-5	1129	291...591	-17	83578	122...491	-6
38	109...043	-1	1428	297...011	-1	114730	593...411	-6
49	225...791	-17	2259	425...023	-1	132269	345...831	-1
53	360...711	-1	2734	415...123	-5	136539	864...023	-1
60	461...451	-1	2828	822...787	-1	147647	599...399	-1
63	368...943	-1	3148	175...227	-5	167068	120...027	-5
65	147...007	-1	3230	849...483	-1	167950	388...883	-5
77	604...191	-1	3779	156...127	-1	257298	104...179	-1
84	773...531	-1	5537	254...887	-1	342647	423...399	-1
87	618...703	-1	5759	171...279	-1	414349	120...207	-5
100	507...507	-5	7069	382...207	-5	418033	118...831	-17
109	259...207	-5	7189	508...207	-5	470053	451...407	-5
147	713...023	-1	7540	233...107	-5	475757	536...791	-1
170	598...611	-1	7729	183...591	-111	483244	347...667	-5
213	526...239	-1	9247	168...687	-5	680337	279...759	-1
235	220...519	-17	10484	398...747	-1	810653	295...711	-1
287	994...999	-1	15795	234...023	-1	857637	115...519	-1

5.2. **Searching for prime values of J_k.** While one can directly apply Algorithm 5.1 to any particular J_k, when searching a large range $1 \le k \le n$ for prime values of J_k it is more efficient to first *sieve* the interval $[1, n]$ to eliminate values of k for which J_k cannot be prime.

For example, as noted in Lemma 4.5, if $k \equiv 0 \pmod 8$ then J_k is divisible by 3. More generally, for any small prime ℓ, one can very quickly compute $J_k \bmod \ell$ for all $k \le n$ by applying the linear recurrence (4) for J_k, working modulo ℓ. If $\ell < \sqrt{n}$, then the sequence $J_k \bmod \ell$ will necessarily cycle, but in any case it takes very little time to identify all the values of $k \le n$ for which J_k is divisible by ℓ; the total time required is just $\tilde{O}(n \log \ell)$, versus $\tilde{O}(n^2)$ if one were to instead apply a trial division by ℓ to each J_k.

We used this approach to sieve the interval $[1, n]$ for those k for which J_k is not divisible by any prime $\ell \le L$. Of course one still needs to consider $J_k \le L$, but this is a small set consisting of roughly $\log_2 L$ values, each of which can be tested very quickly. With $n = 10^6$ and $L = 2^{35}$, sieving reduces the number of potentially prime J_k by a factor of more than 10, leaving 93,707 integers J_k as candidate primes to be tested with Algorithm 5.1. The prime values of J_k found by the algorithm are listed in Table 4, along with the corresponding value of a. As noted in the introduction, we have also proved J_k prime for $k = 1{,}111{,}930$.

The data in Table 4 suggests that prime values of J_k may be more common than prime values of Mersenne numbers M_n; there are 78 primes J_k with fewer than one million bits, but only 33 Mersenne primes in this range. This can be at least partly explained by the fact that M_n can be prime only when n is prime, whereas the values of k for which J_k can be prime are not so severely constrained. By analyzing these constraints in detail, it may be possible to give a heuristic estimate for the density of primes in the sequence J_k, but we leave this to a future article.

References

[1] M. Agrawal, N. Kayal, N. Saxena, *Primes is in P*, Annals of Math. **160** (2004) 781–793.

[2] A. O. L. Atkin, F. Morain, *Elliptic curves and primality proving*, Mathematics of Computation **61** (1993) 29–68.

[3] W. Bosma, *Primality testing with elliptic curves*, Doctoraalscriptie Report 85–12, Department of Mathematics, University of Amsterdam, 1985, `http://www.math.ru.nl/~bosma/pubs/PRITwEC1985.pdf`.

[4] C. Caldwell, *The prime pages: prime number research, records, and resources*, web site at `http://primes.utm.edu/`, 2012.

[5] D. V. Chudnovsky, G. V. Chudnovsky, *Sequences of numbers generated by addition in formal groups and new primality and factorization tests*, Adv. in Appl. Math **7** no. 4 (1986) 385–434.

[6] R. Crandall, C. Pomerance, *Prime numbers: A computational perspective*, Second edition, Springer, New York, 2005.

[7] R. Denomme, G. Savin, *Elliptic purve primality tests for Fermat and related primes*, Journal of Number Theory **128** (2008) 2398–2412.

[8] G. Everest, A. van der Poorten, I. Shparlinski, T. Ward, *Recurrence sequences*, Mathematical Surveys and Monographs **104**, Amer. Math. Soc., Providence, RI, 2003.

[9] Free Software Foundation, *GNU Multiple Precision Arithmetic Library*, version 5.0.1, `http://gmplib.org/`, 2011.

[10] J. von zur Gathen, J. Gerhard, *Modern computer algebra*, second edition, Cambridge University Press, 2003.

[11] S. Goldwasser, J. Kilian, *Almost all primes can be quickly certified*, STOC '86 Proceedings of the Eighteenth Annual ACM Symposium on the Theory of Computing (1986) 316–329.

[12] S. Goldwasser, J. Kilian, *Primality testing using elliptic curves*, J. ACM **46** (1999) 450–472.

[13] D. M. Gordon, *Pseudoprimes on elliptic curves*, in Théorie des nombres (Quebec, PQ, 1987), de Gruyter, Berlin, 1989, 290–305.

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

[15] A. Gurevich, B. Kunyavskiĭ, *Primality testing through algebraic groups*, Arch. Math. (Basel) **93** (2009) 555–564.

[16] A. Gurevich, B. Kunyavskiĭ, *Deterministic primality tests based on tori and elliptic curves*, Finite Fields and Their Applications **18** (2012) 222–236.

[17] O. Katsuyuki, K. Hiroyuki, S. Kouichi, *Elliptic curves with the Montgomery-form and their cryptographic applications*, Public Key Cryptography 2000, LNCS **1751** 238–257, Springer, 2000.

[18] D. H. Lehmer, *An extended theory of Lucas' functions*, Annals of Math. **31** (1930) 419–448.

[19] F. Lemmermeyer, *Reciprocity laws. From Euler to Eisenstein*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000.

[20] H. W. Lenstra Jr., *Elliptic curves and number-theoretic algorithms*, Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Berkeley, Calif., 1986), 99–120, Amer. Math. Soc., Providence, RI, 1987.

[21] H. W. Lenstra Jr., Carl Pomerance, *Primality testing with Gaussian periods*, preprint available at `http://www.math.dartmouth.edu/~carlp/aks041411.pdf`, 2011.

[22] R. L. Lidl, H. Niederreiter, *Introduction to finite fields and their applications*, revised edition, Cambridge University Press, 1994.

[23] J. S. Milne, Elliptic curves, BookSurge Publishers, Charleston, SC, 2006, `http://www.jmilne.org/math/Books/ectext0.pdf`.
[24] P. L. Montgomery, *Modular multiplication without trial division*, Mathematics of Computation **44** (1985) 519–521.
[25] P. L. Montgomery, *Speeding the Pollard and elliptic curve methods of factorization*, Mathematics of Computation **48** (1987) 243–264.
[26] F. Morain, *Elliptic curves, primality proving, and some titanic primes*, Journées Arithmétiques, 1989 (Luminy, 1989), Astérisque No. 198–200 (1991), 245–251 (1992).
[27] F. Morain, *Implementing the asymptotically fast version of the elliptic curve primality proving algorithm*, Mathematics of Computation **76** (2007) 493–505.
[28] T. Pépin, *Sur la formule* $2^{2^n}+1$, Comptes Rendus Acad. Sci. Paris **85** (1877) 329–333.
[29] C. Pomerance, *Very short primality proofs*, Mathematics of Computation **48** (1987) 315–322.
[30] C. Pomerance, *Primality testing: variations on a theme of Lucas*, Congr. Numer. **201** (2010) 301–312.
[31] V. Pratt, *Every prime has a succinct certificate*, SIAM J. Computing **4** (1975) 214–220.
[32] A. Schönhage, V. Strassen, *Schnelle Multiplikation großer Zahlen*, Computing **7** (1971) 281–292.
[33] J. P. Serre, *A course in arithmetic*, Graduate Texts in Mathematics, vol. 7, Springer-Verlag, New York-Heidelberg, 1973.
[34] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.
[35] H. M. Stark, *Counting points on CM elliptic curves*, The Rocky Mountain Journal of Mathematics **26** No. 3 (1996) 1115–1138.
[36] W. A. Stein et al., *Sage Mathematics Software (Version 4.7.1)*, The Sage Development Team, 2011, `http://www.sagemath.org`.
[37] Y. Tsumura, *Primality tests for* $2^p+2^{\frac{p+1}{2}}+1$ *using elliptic curves*, Proceedings of the American Mathematical Society **139** (2011) 2697–2703.
[38] S. Y. Yan, Glyn James, *Testing Mersenne primes with elliptic curves*, in Computer algebra in scientific computing, 303–312, Lecture Notes in Comput. Sci. **4194**, Springer, Berlin, 2006.
[39] A. C. Yao, *On the evaluation of powers*, SIAM J. Computing **5** (1976) 100–103.

Department of Mathematics, University of California, Irvine, CA 92697
E-mail address: `aabatzog@math.uci.edu`

Department of Mathematics, University of California, Irvine, CA 92697
E-mail address: `asilverb@math.uci.edu`

Department of Mathematics, MIT, Cambridge, MA 02139
E-mail address: `drew@math.mit.edu`

Department of Mathematics, University of California, Irvine, CA 92697
E-mail address: `awong@math.uci.edu`