MATHEMATICS OF COMPUTATION
VOLUME 52, NUMBER 185
JANUARY 1989, PAGES 231-245

# On the Number of Elliptic Pseudoprimes

By Daniel M. Gordon

**Abstract.** For an elliptic curve $E$ with complex multiplication by an order in $K = \mathbf{Q}(\sqrt{-d})$, a point $P$ of infinite order on $E$, and any prime $p$ with $(-d \mid p) = -1$, we have that $(p+1) \cdot P = O(\operatorname{mod} p)$, where $O$ is the point at infinity and calculations are done using the addition law for $E$. Any composite number which satisfies these conditions is called an *elliptic pseudoprime*. In this paper it is shown that, assuming the Generalized Riemann Hypothesis, elliptic pseudoprimes are less numerous than primes. In particular, on the GRH, the number of elliptic pseudoprimes less than $x$ is $O(x \log\log x / \log^2 x)$. For certain curves it is shown that infinitely many elliptic pseudoprimes exist.

**1. Introduction.** In [8], the author defined a necessary but not sufficient test for primality, based on the nature of elliptic curves over finite fields. Choose an elliptic curve $E$ with complex multiplication by an order in $K = \mathbf{Q}(\sqrt{-d})$, and a point $P$ on $E$ of infinite order. Then a composite number $n$ is called an *elliptic pseudoprime* if $(-d \mid n) = -1$ and

$$(n+1) \cdot P = O(\operatorname{mod} n). \tag{1.1}$$

These pseudoprimes are analogous to pseudoprimes for Fermat's test (see [19]): composite numbers $n$ for which

$$a^{n-1} \equiv 1 \pmod n$$

for a given $a$. They are also analogous to pseudoprimes for the Lucas-Lehmer test (see [2]): let $D$, $P$ and $Q$ be integers such that $D = P^2 - 4Q \neq 0$ and $P > 0$. Let $U_0 = 0$, $U_1 = 1$, and $U_k = PU_{k-1} - QU_{k-2}$ for $k \geq 2$. Then a composite number $n$ is a *Lucas pseudoprime* if

$$U_{n-(D|n)} \equiv 0 \pmod n.$$

The Lucas-Lehmer test is a degenerate case of the elliptic test (see [8]). For this reason, it seems plausible that the distribution of elliptic pseudoprimes is similar to Fermat and Lucas pseudoprimes. This is supported by empirical data given in Section 3. While that conjecture is still open, this paper will establish (conditional on the Generalized Riemann Hypothesis) an upper bound of $O(x \log\log x / \log^2 x)$ elliptic pseudoprimes less than $x$, which shows that on the GRH they are less numerous than primes (a necessary condition for a compositeness test to be at all useful).

In Section 2, the needed facts about elliptic curves will be presented. In Section 3, basic properties of elliptic pseudoprimes are briefly discussed. The main theorem is

Received October 23, 1987; revised January 15, 1988 and April 27, 1988.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11Y11; Secondary 11Y40, 11A51.

given in Section 4. The paper concludes with a discussion of further open problems concerning elliptic pseudoprimes.

Although the test is not sufficiently better than the Fermat test to be of much practical use, there are several reasons to study elliptic pseudoprimes. They are interesting in their own right as a special set of numbers similar to Fermat and Lucas pseudoprimes, but different enough to require further analysis. A better understanding of them could conceivably lead to stronger compositeness tests, or perhaps a necessary and sufficient condition for primality.

In addition, elliptic curves have become an important tool in computational number theory. Lenstra's factoring algorithm [15] and the Goldwasser-Kilian primality test [7] are two examples. Atkin (see [16]) and Bosma [3] gave different primality tests. Other applications exist in cryptography. Many of the computational properties of elliptic curves are still not well understood, and any new investigation may be useful for other algorithms.

**2. Elliptic Curves with Complex Multiplication.** Let $E$ be the elliptic curve defined by the equation

$$Y^2 = X^3 + AX + B \tag{2.1}$$

for any integers $A, B$ such that $4A^3 + 27B^2 \neq 0$. For any prime $p > 3$, $E_p$ will be the set of all points on this curve over $\mathbf{F}_p$: all pairs $(X, Y)$ which satisfy Eq. (2.1) modulo $p$, together with the point at infinity, $O$. These points form an abelian group with the point at infinity as its identity element. Let $P_1 = (X_1, Y_1)$ and $P_2 = (X_2, Y_2)$. If $P_2 = -P_1$ (i.e., $(X_2, Y_2) = (X_1, -Y_1)$), then $P_1 + P_2 = O$. Otherwise, let

$$\begin{aligned} m &= (Y_2 - Y_1)/(X_2 - X_1) \quad \text{if } P_1 \neq P_2, \\ m &= (3X_1^2 + A)/2Y_1 \quad \text{if } P_1 = P_2. \end{aligned}$$

Then the addition law (see [15], [22]) states that $P_1 + P_2 = (X_3, Y_3)$, where

$$X_3 = -X_1 - X_2 + m^2 \tag{2.2}$$

and

$$Y_3 = -Y_1 + m \cdot (X_1 - X_3).$$

Parametrizations of elliptic curves other than (2.1) may be used, resulting in different addition laws. Montgomery, in [17], gives a parametrization which requires more multiplications but no inversion. Calculations using his version are faster by a constant factor depending on the implementation, since inversions take more time than multiplications.

Hasse proved that $|E_p|$, the order of the elliptic curve, is $p + 1 - a_p$, where $|a_p| \leq 2\sqrt{p}$. Schoof, in [21], gave an algorithm for the computation of $|E_p|$ which runs in time $O((\log p)^9)$. However, the order of elliptic curves with complex multiplication can be more quickly determined.

An elliptic curve is said to have complex multiplication by a field $K = \mathbf{Q}(\sqrt{-d})$ if $\mathrm{End}(E)$, the group of endomorphisms of the curve over $\mathbf{C}$, is an order in the imaginary quadratic field $K$. For a curve defined over $\mathbf{Q}$ with complex multiplication by $K$, the order of $E_p$ is $p + 1$ if $p$ does not split in $K$. If $p$ does split, say

$p = \pi\bar{\pi}$, then the order is $p + 1 - \mathrm{tr}(u\pi)$, where $u$ is some unit in the field and tr denotes the trace.

This reduces the problem of finding the order to determining which unit is the correct one, out of six choices (for $\mathbf{Q}(\sqrt{-3})$), four choices (for $\mathbf{Q}(\sqrt{-1})$), or two choices in all other cases. Lenstra [16] gives methods to determine the correct unit for the first two cases. Which choice is correct can be determined for any curve using class field theory, but in practice for the other cases it is easier to just calculate $(p + 1 + \mathrm{tr}(\pi))P$ and $(p + 1 - \mathrm{tr}(\pi))P$ and see which one is the identity.

As an example, consider curves of the form

$$Y^2 = X^3 - DX. \tag{2.3}$$

These curves have complex multiplication by $\mathbf{Q}(\sqrt{-1})$: the endomorphism corresponding to $i$ sends a point $(X, Y)$ to $(-X, iY)$. A prime $p$ splits in this field if $p \equiv 1 \pmod 4$. Thus, for any of these curves, if $p \equiv 3 \pmod 4$, $|E_p| = p + 1$. Otherwise, we can factor $p$ as $(c + id)(c - id)$, so $\pi = c + id$, and $|E_p| = p + 1 \pm 2c$ or $p + 1 \pm 2d$, corresponding to the units $u = \pm 1$, $\pm i$.

In general, $p$ splits in $\mathbf{Q}(\sqrt{-d})$ if $(-d \mid p) = 1$. If it does split, there are four possible orders if $d = 1$ (corresponding to the units $\pm 1, \pm i$), six if $d = 3$ (corresponding to the sixth roots of unity), and two ($1$ and $-1$) in all other cases. If $p$ is inert, the order will be $p + 1$.

## 3. Elliptic Pseudoprimes.

In this paper we consider a compositeness test: one which, given any number, returns either "composite" or "probably prime." It uses the case of $p$ not splitting in $K$, for which the order of the curve is always $p+1$ if $p$ is prime. The test for any $n$ in the right congruence class is to see if the order of $P$ on $E_n$ divides $n + 1$, i.e., $n$ satisfies Eq.(1.1).

Repeated doublings and additions may be used to calculate $(n+1)P$. An addition chain is a string of integers $a_0, a_1, \ldots, a_r$, where $a_0 = 1$, $a_r = n+1$, and $a_i = a_j + a_k$, for some $j$ and $k$ less than $i$, for all $i = 1, 2, \ldots, r$. Given any such addition chain, $(n + 1)P$ may be calculated by computing $a_iP = a_jP + a_kP$ for $i = 2, 3, \ldots, r$. The final answer does not depend on the addition chain used, but during the inversion step a factor of $n$ may be discovered.

For example, consider the curves $Y^2 = X^3 - DX$. Primes split in $\mathbf{Q}(\sqrt{-1})$ if $p \equiv 1 \pmod 4$, so the test will only be applied to $n \equiv 3 \pmod 4$. If $n$ is composite, finding a point on the curve is difficult, so instead we will only use curves with a rational point. Any point of infinite order will do; while no effectively computable algorithm is known for finding them, algorithms such as the one given by Zagier in [27] work very well in practice.

*Definition.* For an elliptic curve $E$ defined over $\mathbf{Q}$ with complex multiplication by an order in $K = \mathbf{Q}(\sqrt{-d})$, a rational point $P$ of infinite order, and an addition chain for $n + 1$, $n$ is an *elliptic pseudoprime* if $(-d \mid n) = -1$ and $(n + 1)P = O$.

The dependence on the addition chain may be eliminated by using a parametrization for which the addition law has no divisions. The definition may also be extended to curves defined over extensions of $\mathbf{Q}$ (which is necessary for complex multiplication by fields without unique factorization), but in this paper we will only look at curves over $\mathbf{Q}$.

TABLE 1

*Sample curves for pseudoprime tests*

| curve | $j$ | $P$ | $K$ | test for |
|---|---|---|---|---|
| $Y^2 = X^3 - 5X$ | 1728 | (5, 10) | $\mathbf{Q}(\sqrt{-1})$ | $n \equiv 3 \pmod 4$ |
| $Y^2 = X^3 - 120X - 448$ | 8000 | (64, 504) | $\mathbf{Q}(\sqrt{-2})$ | $n \equiv 5, 7 \pmod 8$ |
| $Y^2 = X^3 + 3$ | 0 | (1, 2) | $\mathbf{Q}(\sqrt{-3})$ | $n \equiv 2 \pmod 3$ |
| $Y^2 = X^3 - 3500X - 98000$ | $-3375$ | (84, 448) | $\mathbf{Q}(\sqrt{-7})$ | $n \equiv 3, 5, 6 \pmod 7$ |
| $Y^2 = X^3 - 1056X + 13552$ | $-32768$ | (33, 121) | $\mathbf{Q}(\sqrt{-11})$ | $n \equiv 2, 6, 7, 8, 10 \pmod{11}$ |
| $Y^2 = X^3 - 2432X - 46208$ | $-2^{15} \cdot 3^3$ | (57, 19) | $\mathbf{Q}(\sqrt{-19})$ | $n \neq \Box \pmod{19}$ |
| $Y^2 = X^3 - 495360X - 134193024$ | $-2^{18} \cdot 3^3 \cdot 5^3$ | (817, 2537) | $\mathbf{Q}(\sqrt{-43})$ | $n \neq \Box \pmod{43}$ |
| $Y^2 = X^3 - 117920X + 15585808$ | $-2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$ | (201, 67) | $\mathbf{Q}(\sqrt{-67})$ | $n \neq \Box \pmod{67}$ |
| $Y^2 = X^3 - 34790720X + 78984748304$ | $-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$ | (3400, 548) | $\mathbf{Q}(\sqrt{-163})$ | $n \neq \Box \pmod{163}$ |

Table 1 gives a list of suitable curves, along with integral points, for each field of complex multiplication with class number one.

Each curve can only be used for half of the integers, but using a sufficiently large table of suitable curves would reduce this problem. Only one number in 512 would not be testable by any of the curves in Table 1.

Table 1 contains one curve with complex multiplication by each of the nine fields with class number one [23]. The test would be similar for curves with complex multiplication by fields with class number two or higher, except that these curves would be defined over extensions of $\mathbf{Q}$ and the multiple of $P$ to be calculated would be larger. Since the degree of the extension is equal to the class number of the field, extending the list would best be done by first including curves for each of the 18 fields with class number two, then class number three, and so on, to keep the calculations as manageable as possible.

A composite number $n$ is an elliptic pseudoprime only if $(n+1)P \equiv O \pmod p$ for all primes $p$ dividing $n$ (i.e., the order of $P \bmod p$ divides $n+1$). For any field of complex multiplication, half of the primes will split, and half will be inert. If any prime factor $p$ of $n$ splits in one field and is inert in another, the curves $\bmod p$ for each field will have different orders. Thus the chance of Eq. (1.1) holding for several curves with different fields for any one $n$ is, at least heuristically, very small.

In the calculations summarized in Table 2 below, a standard doubling and multiplying algorithm was used, scanning the digits of the binary representation of $n+1$ from left to right to form the addition chain (see [12]). This method has the advantage that it corresponds to a strong pseudoprimality test. If $n$ is an elliptic pseudoprime and $n+1 = 2^s \cdot d$, where $d$ is odd, call $n$ a *strong elliptic pseudoprime* if

(i) $d \cdot P = O$, or

(ii) $(d \cdot 2^r)P =$ a 2-division point, for some $r$ with $0 \le r < s$.

For elliptic curves given by Eq. (2.1), the 2-division points (points $P$ such that $2 \cdot P = O$) are of the form $(X, 0)$, where $X$ is a root of $X^3 + AX + B \equiv 0 \pmod p$. The left-to-right scan calculates all points of the form $((n+1)/2^j) \cdot P$, and if one of these points is a 2-division point modulo $p$, for some prime factor $p$ of $n$, but is not a 2-division point modulo another prime factor, then the $y$-coordinate of the point is divisible by $p$, and so $n$ will be partially factored during the inversion step in the next doubling.

Numbers up to $10^8$ were tested, with the following results:

TABLE 2

*Number of strong elliptic pseudoprimes up to $x$*

| | | | | | | $x =$ | | |
|---|---|---|---|---|---|---|---|---|
| curve | $K$ | $P$ | $10^3$ | $10^4$ | $10^5$ | $10^6$ | $10^7$ | $10^8$ |
| $Y^2 = X^3 - 13$ | $\mathbf{Q}(\sqrt{-3})$ | $(17, 70)$ | 0 | 1 | 5 | 25 | 59 | 160 |
| $Y^2 = X^3 - 2$ | $\mathbf{Q}(\sqrt{-3})$ | $(3, 5)$ | 0 | 5 | 12 | 33 | 81 | 211 |
| $Y^2 = X^3 + 3$ | $\mathbf{Q}(\sqrt{-3})$ | $(1, 2)$ | 0 | 1 | 3 | 14 | 48 | 138 |
| $Y^2 = X^3 - 5X$ | $\mathbf{Q}(\sqrt{-1})$ | $(5, 10)$ | 0 | 3 | 5 | 19 | 49 | 124 |

These results are consistent with the conjecture that the counting functions for pseudoprimes, Lucas pseudoprimes, and elliptic pseudoprimes are all about the same order (see figures for strong pseudoprimes in [19] and Lucas pseudoprimes in [2]). All of the tests are outdone by the test of Adams and Shanks [1], which detects all but two composite numbers less than $10^8$, and all but 55 less than $50 \cdot 10^9$ [13].

Combining two compositeness tests which are not dependent usually results in a very strong test. In [19] a combination of the Fermat test with base 2 and a Lucas test detected all composites less than $25 \cdot 10^9$. No number less than $10^8$ was an elliptic pseudoprime for all three curves with complex multiplication by $\mathbf{Q}(\sqrt{-3})$. No $n \equiv 11 \pmod{12}$ less than $2 \cdot 10^8$ was an elliptic pseudoprime for both $Y^2 = X^3 + 3$ and $Y^2 = X^3 - 5X$.

**4. An Upper Bound for the Number of Elliptic Pseudoprimes.** For a compositeness test to be useful, pseudoprimes must be rare. This is shown (conditionally) by:

THEOREM 1 (under the Generalized Riemann Hypothesis). *For a fixed elliptic curve $E$ over $\mathbf{Q}$ with complex multiplication by an order in a complex quadratic field $K = \mathbf{Q}(\sqrt{-d})$ and rational point $P$ on $E$ of infinite order, the number of pseudoprimes less than $x$ is $O(x \log\log x / \log^2 x)$.*

Thus, given the GRH, the number of elliptic pseudoprimes less than $x$ is smaller than the number of primes. The proof will follow that of Erdös [6] for pseudoprimes for base 2, with some complications due to the nature of elliptic curves, which force the assumption of the GRH and the weaker bound. Erdös showed that the number of pseudoprimes for base two is less than

$$x \cdot R(x)^{-c_1} \tag{4.1}$$

for some $c_1 > 0$, where

$$R(x) = \exp(\sqrt{\log x \log\log x}).$$

Pomerance, in [18], proved a stronger bound, that the number of pseudoprimes for base two less than $x$ is at most

$$x \cdot L(x)^{-1/2},$$

where

$$L(x) = \exp(\log x \log\log\log x / \log\log x).$$

Pomerance conjectured that the correct order is $x \cdot L(x)^{-1+o(1)}$. It seems likely that the number of pseudoprimes for a fixed base and the number of elliptic pseudoprimes have the same order, but the variable order of elliptic curves mod $p$ makes different means of proof necessary.

The elliptic version of a Carmichael number is an $n$ and $E$ for which $n$ is an elliptic pseudoprime for every point $P$ on $E$. In [8], a heuristic argument is given for the following conjecture.

CONJECTURE 1. *For any $E$ with complex multiplication, the number of elliptic Carmichael numbers less than $x$ is $x \cdot L(x)^{-1+o(1)}$.*

The heuristic argument for this conjecture is similar to the one for pseudoprimes given in [19] and strengthened in [18].

Before proving the theorem, two lemmas are needed. Let $e_p$ denote the order of $P$ on $E_p$.

LEMMA 1. *For a given elliptic curve $E$ and point $P$ of infinite order, the number of primes $p$ such that $e_p = t$ is $O(t^2)$.*

*Proof.* The $n$-division points of $E$ are all points $P$ over $\mathbf{C}$ for which $nP = O$. It is well known that there are $n^2$ such points. The division polynomial $\psi_n(X, Y)$ has roots at all of these points except for those with $2P = O$. $\psi_n$ is discussed in more detail in Section 5.

A point $P = (X, Y)$ has order $t$ over $\mathbf{F}_p$ if and only if $p$ divides $\psi_t(X, Y)$, and $p$ does not divide $\psi_s(X, Y)$ for any $s < t$. Since the degree of $\psi_t(X, Y)$ as a polynomial in $X$ and $Y$ is less than $t^2/2$, $\psi_t = O(c^{t^2})$, where $c$ is a constant depending on $P$ (see Lemma 7 below), and so $\psi_t(X, Y)$ can have at most $O(t^2)$ prime factors. □

LEMMA 2 (ERDÖS [6]). *Let $N(p_1, p_2, \dots, p_k; x)$ denote the number of integers less than $x$, all of whose prime factors come from $p_1, p_2, \dots, p_k$. Put $k^u = x$. Then for $u < \log x / \log\log x$ (i.e., $k > \log x$),*

$$N(p_1, p_2, \dots, p_k; x) < x \cdot \exp(-c_2 u \log u),$$

*where $c_2 > 0$ is an absolute constant.*

Now to prove Theorem 1, choose any $\delta$ with $0 < \delta < 1/4$, and split the elliptic pseudoprimes $n < x$ into four (possibly overlapping) classes:

(i) for every prime $p \mid n$, $e_p \leq R(x)$,

(ii) there is a prime $p \mid n$ with $e_p > R(x)$ and $p$ is inert in $K$,

(iii) there is a prime $p \mid n$ with $e_p \geq x^{1-\delta}$ and $p$ splits in $K$,
(iv) there is a prime $p \mid n$ with $x^{1-\delta} > e_p > R(x)$ and $p$ splits in $K$.

By Lemma 1, the number of primes $p$ with $e_p \leq R(x)$ is at most

$$O\left(\sum_{t \leq R(x)} t^2\right) = O(R(x)^3).$$

Therefore, using Lemma 2 with $k = R(x)^3$, so that $u = c_3(\log x/\log\log x)^{1/2}$, the number of elliptic pseudoprimes in class (i) is at most

$$x \cdot R(x)^{-c_4},$$

for some $c_4 > 0$.

The other classes consist of elliptic pseudoprimes $n$ having at least one prime factor $p$ with $e_p > R(x)$. Since $n$ is an elliptic pseudoprime, we have

$$n \equiv 0 \pmod{p}, \qquad n \equiv -1 \pmod{e_p}. \tag{4.2}$$

Note that $e_p$ and $p$ are relatively prime, since otherwise the two congruences would be contradictory. Therefore, the number of elliptic pseudoprimes $n < x$ with $p \mid n$ is at most

$$1 + \frac{x}{pe_p}.$$

If $p$ is inert in $K$, we have the solution $n = p$, so there are at most $x/(pe_p)$ composite solutions. Therefore, the number of elliptic pseudoprimes in class (ii) is at most

$$\sum_{\substack{p<x \\ e_p > R(x)}} \frac{x}{pe_p} \ll \frac{x \log\log x}{R(x)}. \tag{4.3}$$

Now suppose $p$ splits in $K$ and $n = kp$ for some $k > 1$. Then $p \equiv -1 + a_p \pmod{e_p}$, since $e_p \mid |E_p| = p + 1 - a_p$. Since $a_p \leq 2\sqrt{p}$, for any prime $p$ with $e_p > x^{1-\delta}$ we have that $p \gg x^{1-\delta}$ and $k \gg x^{(1/2)-\delta}$ (since $k \equiv (1-a_p)^{-1} (\operatorname{mod} e_p)$), so the smallest solution to the congruences (4.2) is at least

$$n = kp \gg px^{(1/2)-\delta} \gg x^{(3/2)-2\delta}.$$

This means that for these primes, if $x$ is large enough, the smallest solution will be larger than $x$, and so there will be no elliptic pseudoprimes divisible by $p$ less than $x$. Therefore, class (iii) is empty for $x$ sufficiently large.

The number of elliptic pseudoprimes in class (iv) will be at most

$$\sum_{\substack{p<x \\ p \text{ splits} \\ R(x)<e_p<x^{1-\delta}}} 1 + \frac{x}{pe_p} < \sum_{\substack{p<x \\ p \text{ splits} \\ e_p<x^{1-\delta}}} 1 + \sum_{\substack{p<x \\ p \text{ splits} \\ R(x)<e_p<x^{1-\delta}}} \frac{x}{pe_p}.$$

The second sum is small, as shown in Eq. (4.3), so all that remains to show is that the number of $p < x$ for which $p$ splits in $K$ and $e_p < x^{1-\delta}$ is small. It seems reasonable (but very difficult to prove) that:

CONJECTURE 2. *The number of primes with $e_p < y$ is $O(y^{1+\varepsilon})$ for any $\varepsilon > 0$.*

This conjecture implies a bound as strong as that of Erdös, that the number of elliptic pseudoprimes is at most $x \cdot R(x)^{-c}$. A far weaker lemma suffices to prove the weaker bound of Theorem 1:

LEMMA 3. *Assuming the GRH, the number of primes $p < x$ which split in $K$ and have $e_p < x^{1-\delta}$ is $O(x \log\log x / \log^2 x)$.*

*Proof.* We will look at the index $i_p$ of $P$ in $E_p$, defined by $i_p = |E_p|/e_p$. To prove Lemma 3, we will divide all primes $p < x$ with $e_p < x^{1-\delta}$ into three classes:

$$S_1 = \{p \mid p < x^{1-\delta/2}, e_p \leq x^{1-\delta}\},$$
$$S_2 = \{p \mid x^{1-\delta/2} < p < x, e_p \leq x^{1-\delta} \text{ and } q \mid i_p \rightarrow q < \tfrac{1}{12} \log x\},$$

and

$$S_3 = \{p \mid x^{1-\delta/2} < p < x, e_p \leq x^{1-\delta} \text{ and } q \mid i_p \text{ for some } q \geq \tfrac{1}{12} \log x\}.$$

The first class clearly has size less than $x^{1-\delta/2}$. The other two cases require more effort.

*Size of $S_2$.* From Lemma 3 of Gupta and Murty [9], if $p$ splits in $K$ and $p$ does not divide the discriminant $\Delta$ of $E$, a prime $q$ has $q \mid i_p$ if and only if one of the following is true:

(a) $q$ is inert in $K$ and $p$ splits completely in $K_q$,

(b) $q$ ramifies or splits in $K$, say $q = \alpha_1\alpha_2$, and $\pi_p$ splits completely in $L_{\alpha_1}$ or $L_{\alpha_2}$ or $K_q$.

Here, $K_q = K(E[q])$, the field obtained by adjoining the $q$-division points of $E$ to $K$. $L_\alpha = K(E[\alpha], \alpha^{-1}P)$, where $\alpha^{-1}P$ is a point $B$ on $E$ over $\mathbf{C}$ such that $\alpha \cdot B = P$. We choose $\pi_p$ so that $p = \pi_p\overline{\pi}_p$, and $|E_p| = p + 1 - \operatorname{tr}(\pi_p)$.

For $q$ prime, let $N_q(x)$ denote the number of $p < x$ such that $q \mid i_p$. We estimate $N_q(x)$ for $q < (1/12)\log x$, using an effective version of Chebotarev's Density Theorem:

LEMMA 4 (LAGARIAS AND ODLYZKO [14]). *Let $L/K$ be a normal extension of degree $n$ with discriminant $d_L = \operatorname{disc}(L/\mathbf{Q})$. Let $\pi_C(x, L/K)$ be the number of prime ideals in $K$ unramified in $L$ with norm less than $x$ and Frobenius automorphism in a given conjugacy class $C$ of $\operatorname{Gal}(L/K)$. If the GRH holds for the Dedekind zeta function of $L$, then*

$$\left|\pi_C(x, L/K) - \frac{|C|}{n} Li(x)\right| \ll |C| x^{1/2} \left(\log x + \frac{\log d_L}{n}\right).$$

Returning to the proof of Lemma 3, we apply this result to bound $N_q(x)$, using bounds on the degrees and discriminants of $K_q$, $L_{\alpha_1}$ and $L_{\alpha_2}$. It is shown in Lemma 7 of [9] that for prime $q$ one has

$$\frac{\log d_L}{n} \ll \log q$$

for each of these fields and $[L_{\alpha_i} \colon \mathbf{Q}] \gg q^{3/2}$, $[K_q \colon \mathbf{Q}] \gg q^2$. Then, using (a) and (b) above, Lemma 4 implies the bound

$$N_q(x) \ll \frac{1}{q^{3/2}} \frac{x}{\log x} + x^{1/2} \log q + x^{1/2} \log x.$$

Now let $y = \frac{1}{12}\log x$, and $I(q)$ denote the product over all $p < x$ and $q < y$ of all the powers of $q$ dividing $i_p$. By the above, we have that the log of the product of $i_p$ for all $p \in S_2$ is

$$\begin{aligned} \log \prod_{q<y} I(q) &\ll \log \left( \prod_{q<y} q^{\frac{1}{q^{3/2}}\frac{x}{\log x}+x^{1/2}\log q+x^{1/2}\log x} \right) \\ &\ll \frac{x}{\log x}\sum_{q<y}\frac{\log q}{q^{3/2}}. \end{aligned} \tag{4.4}$$

The sum is convergent, and so the whole expression is less than $cx/\log x$ for some absolute constant $c$.

Suppose now that at least $dx/\log^2 x$ primes all have $e_p < x^{1-\delta}$. Then by the definition of $S_2$,

$$i_p > \frac{p+1-2\sqrt{p}}{e_p} > \frac{\frac{1}{2}x^{1-\delta/2}}{x^{1-\delta}} = \frac{1}{2}x^{\delta/2},$$

and so

$$\log \prod_{q<y} I(q) \geq \log \left( \prod_{p\in S_2} i_p \right) \geq \log \left( \frac{1}{2}x^{\delta/2} \right)^{dx/\log^2 x} \geq \frac{\delta}{3}\frac{dx}{\log x} \tag{4.5}$$

for $x$ sufficiently large. By choosing $d$ large enough, this contradicts (4.4). Thus, $|S_2| \ll x/(\log x)^2$.

*Size of* $S_3$. In Section 6 of [9], Gupta and Murty define the quantity

$$M(y_1, y_2) = |\{p \mid p < x \text{ and } q \mid i_p \text{ for some } y_1 < q < y_2\}|.$$

They show, assuming the GRH, a result which implies

$$M(y, 2x) = O\left(\frac{x\log\log x}{\log^2 x}\right).$$

$S_3$ is clearly contained in the set counted by $M(y, 2x)$, and so the number of primes $p < x$ with $e_p < x^{1-\delta}$ is at most $|S_1| + |S_2| + |S_3| = O(x\log\log x/\log^2 x)$. □

The condition in Theorem 1 that the curve is defined over **Q** is used in the proof of Lemma 3, both in the estimates of degrees and discriminants and the lemmas from [9], which deal only with the class number one case. The same theorem can be shown for curves over extensions $K$ of **Q**, but the implied constant in the bound would strongly depend on the field $K$.

**5. Lower Bounds and Other Open Problems.** It seems to be a hard problem to establish a good lower bound for the number of elliptic pseudoprimes. Unfortunately, the various methods used in [2], [11], [18] and [19] to give lower bounds for pseudoprimes all run into difficulties when applied to elliptic pseudoprimes.

To consider lower bounds, it is convenient to use a parametrization of the elliptic curve for which the addition law has no divisions, as in [17]. In this case, no pseudoprimes are eliminated by the inversion step, simplifying the analysis.

We will prove that an infinite number of elliptic pseudoprimes exist for certain curves by using the properties of the division polynomial $\psi_n(X,Y)$. A number of facts about elliptic functions will be needed. For proofs, see [24], [4] or [5].

Recall that the division polynomial $\psi_n(X,Y)$ has roots at the $n$-division points of $E$: $P=(X,Y)$ such that $n\cdot P=O$. These polynomials are often defined by the equations

$$\begin{aligned}
\psi_0(X,Y)&=0,\\
\psi_1(X,Y)&=1,\\
\psi_2(X,Y)&=2Y,\\
\psi_3(X,Y)&=3X^4+6AX^2+12BX-A^2,\\
\psi_4(X,Y)&=4Y(X^6+5AX^4+20BX^3-5A^2X^2-4ABX-8B^2-A^3)
\end{aligned}$$

and the recurrence

$$\psi_{m+n}\psi_{m-n}=\psi_{m-1}\psi_{m+1}\psi_n^2-\psi_{n-1}\psi_{n+1}\psi_m^2. \tag{5.1}$$

These polynomials may also be defined in terms of elliptic functions. Let $L$ be the lattice generated by $\omega_1$ and $\omega_2$ for any complex numbers such that $\operatorname{Im}(\omega_2/\omega_1)>0$. The Weierstrass $\wp$-function is defined by

$$\wp(z)=\frac{1}{z^2}+\sum_{\substack{\omega\in L\\ \omega\neq 0}}\left\{\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2}\right\}.$$

This is an elliptic function which satisfies the relation

$$\wp'^2(z)=4\wp^3(z)-g_2\wp(z)-g_3,$$

where $g_2$ and $g_3$ are functions of $L$. Therefore, if we take $L$ so that $A=-g_2/4$, $B=-g_3/4$, and $z$ to be the point in the period parallelogram $\mathbf{C}/L$ such that $\wp(z)=X$, then $\wp'(z)/2=Y$, and we have a correspondence between complex numbers $z$ in the period parallelogram and points on the curve $E$ over $\mathbf{C}$. The point at infinity corresponds to $z=0$, where $\wp$ has a pole.

Under this map, the addition law on the curve corresponds to complex addition modulo the lattice $L$. The $n$-division points on the curve correspond to the $n^2$ complex numbers $z$ such that $nz\in L$. Let $f_n(z)$ be the function defined on $\mathbf{C}/L$ by $f_n(z)=\psi_n(X,Y)$, where $\wp(z)=X$. As mentioned in the proof of Lemma 1, the roots of $\psi_n$ are the $n$-division points, and so we get another definition of the division polynomials:

$$\psi_n^2(X,Y)=f_n^2(z)=n^2\prod_{nu\in L}(\wp(z)-\wp(u)). \tag{5.2}$$

LEMMA 5. *Let $\omega_1$ and $\omega_2$ be basic periods of $\wp(z)$, and define $\omega_{ab}=a\omega_1+b\omega_2$. Let $\eta_1=\varsigma(\omega_1/2)$ and $\eta_2=\varsigma(\omega_2/2)$, for Weierstrass's $\varsigma$-function, and $\eta_{ab}=a\eta_1+b\eta_2$. Then for the Weierstrass $\sigma$-function:*

$$\sigma(z+\omega_{ab})=(-1)^{a+b}\sigma(z)e^{2\eta_{ab}(z+\omega_{ab}/2)}.$$

*Proof.* This is an extension of the well-known properties of $\sigma(z)$, that

$$\sigma(z+\omega_1) = -\sigma(z)e^{2\eta_1(z+\omega_1/2)}$$

and

$$\sigma(z+\omega_2) = -\sigma(z)e^{2\eta_2(z+\omega_2/2)}.$$

The lemma follows easily by induction on $a$ and $b$. □

LEMMA 6. *We have $\psi_n(X,Y) = \sigma(nz)/\sigma(z)^{n^2}$, where $z$ is the complex number in $\mathbf{C}/L$ for which $\wp(z) = X$.*

LEMMA 7. *For an elliptic curve $E$ and point $P = (X,Y)$ of infinite order, there exists a constant $c > 1$ for which*

$$\psi_n(X,Y) = (1+o(1))c^{n^2}.$$

THEOREM 2. *Suppose $E$ is an elliptic curve with complex multiplication by an order in $K$ and an integral point of infinite order $P = (X,Y)$, and $p$ is a prime which is inert in $K$ and does not divide $\psi_2(X,Y)$. Then*

$$\psi_{2p}(X,Y)/\psi_2(X,Y) \equiv -1 \pmod{p}.$$

*Proof.* Since the order of $P$ on $E_p$ divides $p+1$, we have that $\psi_{p+1}(X,Y) \equiv 0 \pmod{p}$. Let $R = \mathbf{Q}(E[p+1])$ be the field obtained by adjoining all the $(p+1)$-division points on $E$ to the rationals, and $\mathfrak{p}$ be any prime ideal in $R$ dividing $p$. Then $\psi_{p+1}(X,Y) \equiv 0 \pmod{\mathfrak{p}}$, and so by Eq. (5.2) there must be some $(p+1)$-division point $u$ such that $\mathfrak{p} \mid (\wp(z) - \wp(u))$. Since any such point can be written as $\omega_{ab}/(p+1)$ for some $a$ and $b$, we have

$$\wp(z) \equiv \wp\left(\frac{\omega_{ab}}{p+1}\right) \pmod{\mathfrak{p}}.$$

This, and Eq. (5.2), along with the definition of $f_n(z)$, imply that

$$\psi_n(X,Y) \equiv f_n\left(\frac{\omega_{ab}}{p+1}\right) \pmod{\mathfrak{p}}$$

for all $n \geq 0$.

Let $k$ be any integer between 0 and $2p+2$. Then by Lemma 6,

$$\begin{aligned}\psi_{2p+2-k}(X,Y) &\equiv \frac{\sigma((2p+2-k)\omega_{ab}/(p+1))}{\sigma(\omega_{ab}/(p+1))^{(2p+2-k)^2}} \pmod{\mathfrak{p}}\\ &\equiv \frac{(-1)^{2a+2b+1}\sigma(k(\omega_{ab}/(p+1)))e^{4\eta_{ab}(\omega_{ab}-k(\omega_{ab}/(p+1)))}}{\sigma(\omega_{ab}/(p+1))^{k^2}\sigma(\omega_{ab}/(p+1))^{4(p+1)^2-4(p+1)k}} \pmod{\mathfrak{p}}\end{aligned}$$

by Lemma 5. Using Lemma 6, we get

$$\psi_{2p+2-k}(X,Y) \equiv -\psi_k(X,Y)\alpha^{2(k-(p+1))} \pmod{\mathfrak{p}}, \tag{5.3}$$

where

$$\alpha = \frac{\sigma(\omega_{ab}/(p+1))^{2(p+1)}}{e^{2\eta_{ab}\omega_{ab}/(p+1)}}.$$

This is equivalent to Eq. (15.3) in [24]. Since the $\psi_k$'s are integers, letting $k=1$ and 2 in Eq. (5.3) shows that $\alpha^{-2p}$ and $\alpha^{-2p+2}$ are congruent to rational integers mod $\mathfrak{p}$, and so $\alpha^2$ must be equal to a rational integer mod $\mathfrak{p}$. But then all of the quantities in Eq. (5.3) are rational integers mod $\mathfrak{p}$, and so the congruence must hold modulo $p$.

For $k = 2$, this gives

$$\psi_{2p}(X,Y) \equiv -\psi_2(X,Y)(\alpha^{-2})^{p-1} \equiv -\psi_2(X,Y) \pmod{p}. \quad \square$$

Although Theorem 2 will suffice to show that there are an infinite number of elliptic pseudoprimes for certain curves, other properties of the division polynomials need to be better understood to strengthen the results. For example, by similar manipulations, it may be shown that

$$\psi_{p+1-k}(X,Y) \equiv (-1)^{a+b+1}\psi_k(X,Y)\alpha^{k-(p+1)/2} \pmod{p}.$$

From this it follows that $\alpha$ is equal to an integer mod $p$. Letting $k = 1$, we get

$$\psi_p(X,Y) \equiv (-1)^{a+b+1}\alpha^{(p-1)/2} \pmod{p}.$$

This shows that $\psi_p(X,Y) \equiv \pm 1 \pmod{p}$ for inert primes $p$. In fact, $\psi_p(X,Y)$ is always equal to $-1 \pmod{p}$, but a proof requires use of the facts that a supersingular curve has a trivial group of $p$-torsion points over $\mathbf{F}_p$ (see [22]). An elementary proof would be interesting, and might help getting stronger lower bounds for elliptic pseudoprimes.

COROLLARY 1. *For a curve $E$ with complex multiplication by an order in $K = \mathbf{Q}(\sqrt{-d})$ and point of infinite order $P = (X,Y)$, let $n = \psi_{2p}(X,Y)/\psi_2(X,Y)$ for any sufficiently large prime $p$. Then $n$ is an elliptic pseudoprime if*

$$\text{(5.4)} \qquad \begin{array}{ll} \text{(i)} & (-d \mid p) = -1, \\ \text{(ii)} & (-d \mid n) = -1, \\ \text{(iii)} & n \equiv 1 \pmod{2}. \end{array}$$

*Proof.* By (i), $p$ is inert in $K$, so by Theorem 2 we have $n \equiv -1 \pmod{p}$. Together with (iii) this implies that $2p$ divides $n + 1$. By the definition of $n$, the point $P$ has order dividing $2p$ on $E_q$ for each of the prime divisors $q$ of $n$, so $(n+1)P \equiv O \pmod{n}$. By (ii), $n$ is in the right congruence class mod $d$ for the pseudoprime test.

The only other necessary condition is that $n$ be composite. This follows from the fact that $\psi_p \mid \psi_{2p}$, and that, by Lemma 7, $\psi_{2p} > \psi_p$ for $p$ large enough, so $\psi_p$ is a *proper* divisor of $\psi_{2p}$. Therefore $n$ is an elliptic pseudoprime.

Alternatively, it can be shown, using results of Ward [26], that for $k$ sufficiently large, $\psi_k(X,Y)$ will always have a primitive prime divisor: a prime $q$ such that $q \mid \psi_k$ and $q$ does not divide $\psi_l$ for any $l < k$. The proof runs along the same lines as the proof of the corresponding theorem for Lehmer numbers in [25]. For $k = 2p$, this also shows that $\psi_{2p} \neq \psi_p$. $\square$

COROLLARY 2. *There are infinitely many elliptic pseudoprimes for the curve $E$: $Y^2 = X^3 + 3$ and point $P = (1,2)$.*

*Proof.* This curve has complex multiplication by $\mathbf{Q}(\sqrt{-3})$, so by Corollary 1, $n$ will be an elliptic pseudoprime for any prime $p \equiv 2 \pmod{3}$ which has $n = \psi_{2p}(1,2)/\psi_2(1,2) \equiv 2 \pmod{3}$ and $n \equiv 1 \pmod{2}$.

The sequence $\phi_k = \psi_{2k}(X,Y)/\psi_2(X,Y)$ for $k = 0, 1, \ldots$ is also an elliptic divisibility sequence: it still satisfies the recurrence (5.1), and if $k$ divides $l$ then $\phi_k$ divides $\phi_l$. Ward shows in [24] that such sequences are periodic modulo any prime; in this case we are interested in 2 and 3. For this curve it turns out that for $p \equiv 5 \pmod 6$, $\psi_{2p}(1,2)/\psi_2(1,2) \equiv 5 \pmod 6$. Therefore, there will be an elliptic pseudoprime for each such prime. Since there are an infinite number of these primes by Dirichlet's Theorem on primes in arithmetic progressions, there are an infinite number of elliptic pseudoprimes for this curve and point. □

Because of the growth rate of the $\psi_k$'s, the pseudoprimes constructed by this method tend to be quite large. For instance, the first pseudoprime from Corollary 1 is

$$\psi_{10}/\psi_2 = 16617839269761894629 = 179 \cdot 61469 \cdot 64951 \cdot 23253029.$$

This method will not work if conditions (i) and (ii) in (5.4) are mutually exclusive, or if $\psi_{2p}(X,Y)/\psi_2(X,Y)$ is always divisible by 2, which happens for most of the curves in Table 1. While it does not work for all curves, it should not be hard to find examples of curves with complex multiplication by each field with class number one for which all three conditions are met infinitely often. For instance, for $\mathbf{Q}(\sqrt{-1})$, the curve $Y^2 = X^3 - 5X$ and point (5,10) is not suitable, but for the curve $Y^2 = X^3 + 3X$ and point (12,42) all three conditions are satisfied for any prime $p \equiv 3 \pmod 4$.

In cases where Corollary 1 applies, we also get a lower bound for the number of elliptic pseudoprimes. For instance, in the curve of Corollary 2, since $\psi_{2p}(X,Y)/\psi_2(X,Y) \ll c^{4p^2}$ by Lemma 7, and the number of primes $\equiv 5 \pmod 6$ less than $x$ is about $\frac{1}{2}\frac{x}{\log x}$, the number of elliptic pseudoprimes less than $x$ obtained by this method is

$$\gg \frac{\sqrt{\log x}}{\log\log x}. \tag{5.5}$$

This is much weaker than the heuristic argument given in [8], which gives a construction for $x \cdot L(x)^{-1+o(1)}$ elliptic pseudoprimes less than $x$, the correct order if Conjecture 1 is correct. However, that argument uses several difficult number-theoretic conjectures, and is not likely to yield any rigorous lower bound.

The bound in (5.5) is also weaker than lower bounds known for Fermat and Lucas pseudoprimes. A deeper understanding of the divisibility properties of the division polynomials is necessary to improve the bound or get a general lower bound for all curves.

There are a number of other open problems regarding elliptic pseudoprimes. One difficult problem is to improve the upper bound, or remove the use of the Generalized Riemann Hypothesis. Another is to get a result analogous to Rabin's in [20]: for any composite number $n$, the fraction of points on an elliptic curve for which $n$ is a strong elliptic pseudoprime is at most some $c < 1$.

Finally, in [8], Euler elliptic pseudoprimes are defined analogously to the regular case: $n$ is an Euler elliptic pseudoprime if $n \equiv 1 \pmod 4$ and

$$\left(\frac{n+1}{2}\right) P = \begin{cases} O, P = 2Q \text{ for some } Q \text{ on } E_n \\ \text{a 2-division point, otherwise.} \end{cases} \tag{5.6}$$

The restriction to $n \equiv 1 \pmod 4$ is to ensure that $E_n$ is cyclic if $n$ is a prime. A simple way to check whether $P$ is twice another point, analogous to the Jacobi symbol, would make this a practical test. For Fermat and Lucas pseudoprimes, all strong pseudoprimes are also Euler pseudoprimes. The proof does not carry over to elliptic pseudoprimes, and it would be interesting to find a strong elliptic pseudoprime $n \equiv 1 \pmod 4$ which does not pass Eq. (5.6), or prove that none exist.

**Acknowledgments.** The author would like to thank Carl Pomerance for many helpful discussions and suggestions. and an anonymous referee for suggesting improvements in the proof of Theorem 1 and the presentation of this paper.

Department of Computer Science
University of Georgia
Athens, Georgia 30602

1. W. W. ADAMS & D. SHANKS, "Strong primality tests that are not sufficient," *Math. Comp.*, v. 39, 1982, pp. 255–300.

2. R. BAILLIE & S. S. WAGSTAFF, JR., "Lucas pseudoprimes," *Math. Comp.*, v. 35, 1980, pp. 1391–1417.

3. W. BOSMA, *Primality Testing Using Elliptic Curves*, Report 85-12, Mathematisch Instituut, Universiteit van Amsterdam, 1985.

4. K. CHANDRASEKHARAN, *Elliptic Functions*, Springer-Verlag, New York, 1985.

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.*, v. 7, 1987, pp. 385–434.

6. P. ERDÖS, "On pseudoprimes and Carmichael numbers," *Publ. Math. Debrecen*, v. 4, 1956, pp. 201–206.

7. S. GOLDWASSER & J. KILIAN, *Almost All Primes Can be Quickly Certified*, Proc. 18th Annual ACM Sympos. on Theory of Computing, 1986, pp. 316–329.

8. D. M. GORDON, *Pseudoprimes on Elliptic Curves*, Proc. Internat. Number Theory Conference, Laval, 1987. (To appear.)

9. R. GUPTA & M. RAM MURTY, "Primitive points on elliptic curves," *Compositio Math.*, v. 58, 1986, pp. 13–44.

10. K. IRELAND & M. ROSEN, *A Classical Introduction to Modern Number Theory*, Graduate Texts in Math., vol. 84, Springer-Verlag, New York, 1982.

11. P. KISS, B. M. PHONG & E. LIEUWENS, "On Lucas pseudoprimes which are the products of $s$ primes," in *Fibonacci Numbers and Their Applications*, Reidel, Dordrecht, 1986, pp. 131–139.

12. D. E. KNUTH, *The Art of Computer Programming*, Vol. 2, 2nd ed., Addison-Wesley, Reading, Mass., 1981.

13. G. KURTZ, D. SHANKS & H. C. WILLIAMS, "Fast primality tests for numbers less than $50 \cdot 10^9$," *Math. Comp.*, v. 46, 1986, pp. 691–701.

14. J. C. LAGARIAS & A. M. ODLYZKO, "Effective versions of the Chebotarev Density Theorem," *Algebraic Number Fields* (A. Frölich, ed.), Academic Press, New York, 1977, pp. 409–464.

→ H. W. LENSTRA, JR., "Factoring integers with elliptic curves," *Ann. of Math.*, v. 126, 1987, pp. 649–673.

16. H. W. LENSTRA, JR., "Elliptic curves and number theoretic algorithms," preprint, 1986.

17. P. L. MONTGOMERY, "Speeding the Pollard and elliptic curve methods of factorization," *Math. Comp.*, v. 48, 1987, pp. 243–264.

18. C. POMERANCE, "On the distribution of pseudoprimes," *Math. Comp.*, v. 37, 1981, pp. 587–593.

19. C. POMERANCE, J. L. SELFRIDGE & S. S. WAGSTAFF, JR., "The pseudoprimes to $25 \cdot 10^9$," *Math. Comp.*, v. 35, 1980, pp. 1003-1026.

→ M. O. RABIN, "Probabilistic algorithm for testing primality," *J. Number Theory*, v. 12, 1980, pp. 128–138.

21. R. SCHOOF, "Elliptic curves over finite fields and the computation of square roots mod $p$," *Math. Comp.*, v. 44, 1985, pp. 483–494.

22. J. H. SILVERMAN, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math., vol. 106, Springer-Verlag, New York, 1986.

23. H. M. STARK, "A complete determination of the complex quadratic fields of class-number one," *Michigan Math. J.*, v. 14, 1967, pp. 1–27.

→ M. WARD, "Memoir on elliptic divisibility sequences," *Amer. J. Math.*, v. 70, 1948, pp. 31–74.

→ M. WARD, "The intrinsic divisors of Lehmer numbers," *Ann. of Math.*, v. 62, 1955, pp. 230–236.

26. M. WARD, "The law of repetition of primes in an elliptic divisibility sequence," *Duke Math. J.*, v. 15, 1948, pp. 941–946.

27. D. ZAGIER, "Large integral points on elliptic curves," *Math. Comp.*, v. 48, 1987, pp. 425–436.