MATHEMATICS OF COMPUTATION
VOLUME 53, NUMBER 187
JULY 1989, PAGES 415–430

Elliptic Pseudoprimes

By Ian Miyamoto and M. Ram Murty*

Abstract. Let E be an elliptic curve over Q with complex multiplication by an order in an imaginary quadratic field. Let ψ_n denote the nth division polynomial, and let P be a rational point of E of infinite order. A natural number n is called an *elliptic pseudoprime* if $n|\psi_{n+1}(P)$ and n is composite. Let $N(x)$ denote the number of elliptic pseudoprimes up to x. We show that $N(x) \ll x(\log\log x)^{7/2}/(\log x)^{3/2}$. More generally, if $P_1, \dots, P_r$ are r independent rational points of E which have infinite order, and Γ is the subgroup generated by them, denote by $N_\Gamma(x)$ the number of composite $n \le x$ satisfying $n|\psi_{n+1}(P_i)$, $1 \le i \le r$. For $r \ge 2$, we prove $N_\Gamma(x) \ll x\exp(-c\sqrt{(\log x)(\log\log x)})$ for some positive constant c.

1. Introduction. The problem of determining whether a given integer is prime or not is very basic to mathematics. Fermat's 'little theorem' provides us with a criterion:

$$\text{for any odd prime } p, \qquad 2^{p-1} \equiv 1 \pmod{p}. \tag{0.1}$$

One may thus test a given n by computing $2^{n-1} \pmod{n}$. If the congruence

$$2^{n-1} \equiv 1 \pmod{n} \tag{0.2}$$

fails, then n is definitely composite. If, however (0.2) is satisfied, all that can be said is that n is *probably* prime. Indeed, there are infinitely many composite numbers that satisfy (0.2). These are called false witnesses or pseudoprimes (to the base 2) and will be denoted psp_2 for short. (More generally, for any odd prime p, $(a,p)=1$, one has $a^{p-1} \equiv 1 \pmod{p}$, so we may likewise define psp_a.) Though there are infinitely many such numbers, their cardinality up to x is substantially smaller than the number of primes up to x. This therefore gives a probabilistic primality test. This test and modifications of it have been studied extensively. (The reader may refer to [5] or [12].)

Indeed, let $P_2(x)$ denote the number of psp_2 up to x. Erdös [3] established that for some positive constants c_1, c_2,

$$c_1 \log x \ll P_2(x) \ll xR(x)^{-c_2}, \tag{1.1}$$

where

$$R(x) = \exp(\sqrt{\log x \log\log x}). \tag{1.2}$$

Pomerance [12] had subsequently improved these bounds to

$$\exp(\log^{5/14} x) \ll P_2(x) \ll xL(x)^{-1/2}, \tag{1.3}$$

Received August 29, 1988.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11G05, 11Y11, 11A51.
*Research supported by NSERC grant A9418.

where

$$L(x) = \exp\left(\log x \log\log\log x / \log\log x\right), \tag{1.4}$$

and has conjectured that this is nearly best possible: the correct order is guessed to be

$$xL(x)^{-1+o(1)}.$$

Recently, elliptic curves have been applied to this problem of distinguishing primes from composites, again, using only the basic theory. Gordon [7], for example, considers such a test which uses curves (with what is known as complex multiplication), that is analogous to the Fermat test described above.

In order to describe the test quickly, we consider a special case. Let E be an elliptic curve with complex multiplication by the ring of Gaussian integers, $Z[i]$. If E has good reduction at p and $p \equiv 3 \pmod 4$, then $E(F_p)$ has size $p+1$. If P is a rational point of E of infinite order, then $(p+1)P = 0$ in $E(F_p)$, provided P has good reduction at p. This is analogous to Fermat's little theorem, and we can utilize this as a primality test for primes $\equiv 3 \pmod 4$. More precisely, we can utilize the division polynomials to give an equivalent formulation of this criterion. Let ψ_n denote the nth division polynomial (as defined in Section 2). The equation $(p+1)P = 0$ in $E(F_p)$ can be rephrased as $p \mid \psi_{p+1}(P)$. We therefore say that a composite number n is an *elliptic pseudoprime* if $n \mid \psi_{n+1}(P)$. Gordon [7] has recently shown that there are infinitely many such pseudoprimes. Assuming a generalized Riemann hypothesis (GRH), he proved [6] that the number of elliptic pseudoprimes up to x is less than

$$\frac{x \log\log x}{(\log x)^2}.$$

This therefore gave a probabilistic primality test using elliptic curves, but only *conditionally.*

The purpose of this paper is to establish this probabilistic primality test *without the use of the generalized Riemann hypothesis.* We do this by showing that the number of elliptic pseudoprimes up to x is

$$\ll \frac{x(\log\log x)^{7/2}}{(\log x)^{3/2}}.$$

In Section 2 we will provide the needed background of elliptic curves in order to describe Gordon's test. In Section 3 we will describe the test and a suitable generalization of the test to elliptic curves of rank ≥ 2. The idea is to consider r independent rational points $P_1, ..., P_r$ on the curve E and let Γ be the group generated by them. Denote by $N_\Gamma(x)$ the number of composite $n \leq x$ satisfying $n \mid \psi_{n+1}(P_i)$, $1 \leq i \leq r$. The case of elliptic pseudoprimes can be viewed as the case $r = 1$. If $r \geq 2$, we are able to obtain a substantially better estimate for $N_\Gamma(x)$. In Sections 4–6 we will prove our main theorems on the number of elliptic pseudoprimes. In case $r \geq 2$, we obtain

$$N_\Gamma(x) \ll xR(x)^{-c},$$

where

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

and c is some positive constant. This upper bound is the same as established for psp_2 by Erdös [3].

The key tool in the derivation is a lemma established by Gupta and Ram Murty [8] and the methods of that paper. This lemma does generalize to elliptic curves over arbitrary number fields, and more generally to abelian varieties. However, the error terms grow large as the degree of the base field increases and therefore the results of this paper do not generalize easily to other number fields.

2. Elliptic Curves. We briefly review the salient features of elliptic curves. For a quick survey, the reader should consult Tate [14] and for a detailed treatment, Silverman [13] is ideal.

Let k be a field. An elliptic curve E defined over k may be thought of as the zero set of a plane algebraic curve given in affine coordinates by

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2.1}$$

where the $a_i \in k$. (In projective space, E is defined by a nonsingular homogeneous cubic polynomial.) If the characteristic of k is not 2 or 3, E has a simpler model of the form

$$E\colon y^2 = x^3 + ax + b. \tag{2.2}$$

A simple calculation shows that the nonsingularity of E is equivalent to the fact that

$$\Delta = -16(4a^3 + 27b^2) \neq 0.$$

This number is called the discriminant of E and is -16 times the discriminant of the polynomial

$$x^3 + ax + b.$$

It is well known that multiplication by m is a map of degree m^2. One may see this in many ways. One method is by using explicit formulas. Indeed, using the addition law, one can define division polynomials,

$$\{\psi_n\}_{n=1}^{\infty}. \tag{2.3}$$

Each $\psi_n(x, y)$ is in $k[x, y]$ and has zeros exactly at the n-division points of $E(\overline{k})$. (Here $\overline{k}$ is the algebraic closure of k.) These polynomials may be defined by [1]:

$$\begin{cases} \psi_1 = 1, \\ \psi_2 = 2y, \\ \psi_3 = 3x^4 + 6ax^2 + 12bx - a^2, \\ \psi_4 = 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3) \end{cases} \tag{2.4}$$

and the recursive relation,

$$\psi_{m-n}\psi_{m+n} = \psi_{m-1}\psi_{m+1}\psi_n^2 - \psi_{n-1}\psi_{n+1}\psi_m^2. \tag{2.5}$$

By setting $m = n + 1$ in (2.5) we find that

$$\psi_{2n+1} = \psi_n^3\psi_{n+2} - {\psi_{n+1}}^3\psi_{n-1},$$

and by setting $m = n + 2$,

$$2y\psi_{2n} = \psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2).$$

Further, we define

$$\begin{aligned} \phi_m &= x\psi_m^2 - \psi_{m-1}\psi_{m+1}, \\ 4y\omega_m &= \psi_{m+2}{\psi_{m-1}}^2 - \psi_{m-2}{\psi_{m+1}}^3. \end{aligned} \tag{2.6}$$

It follows that for m odd, $\phi_m, y^{-1}\omega_m, \psi_m$, and for m even, $(2y)^{-1}\psi_m, \phi_m^2, \omega_m$ are all polynomials in $k[a,b,x]$. Moreover, ϕ_m is monic, and ϕ_m and ψ_m^2 are relatively prime of degree m^2 and $m^2 - 1$, respectively, and

$$[m]P = \left(\frac{\phi_m}{\psi_m^2}, \frac{\omega_m}{\psi_m^3}\right). \tag{2.7}$$

For m odd, ψ_m^2 has zeros exactly at the m-division points of E and, being of degree $m^2 - 1$, we see that the degree of $[m]$ is m^2. (Do not forget that $[m]\mathcal{O} = \mathcal{O}$.)

Let $\operatorname{End}_k E$ denote the ring of endomorphisms of E defined over k. If $\bar{k}$ denotes the algebraic closure of k, the above considerations show that $\operatorname{End}_{\bar{k}} E \supseteq Z$. If k has characteristic zero, it is known that $\operatorname{End}_{\bar{k}} E = Z$ or is an order in an imaginary quadratic field $K = Q(\sqrt{-d})$. If $\operatorname{End}_{\bar{k}} E \neq Z$, then E is said to have complex multiplication (CM) by an order in K (or more briefly, by K).

If E is defined over Q, and has CM by K, then necessarily K has class number 1, so is one of the nine fields, $K = Q(\sqrt{-d})$ with

$$d = 1, 2, 3, 7, 11, 19, 43, 67, 163.$$

Up to isomorphism over $\bar{Q}$, there are only thirteen elliptic curves with CM by an order in one of these fields. Nine of these isomorphism classes of curves have CM by the full ring of integers, and four others have

$$\begin{aligned} K = Q(\sqrt{-1}), Q(\sqrt{-3}), Q(\sqrt{-7}) \quad &\text{with} \quad \operatorname{End} E = Z + 2O_K, \\ K = Q(\sqrt{-3}) \quad &\text{with} \quad \operatorname{End} E = Z + 3O_K. \end{aligned}$$

Each class, of course, contains infinitely many curves. For example, $j = 1728$ gives all the curves $E\colon y^2 = x^3 + Dx$.

3. The Test.

Let E be an elliptic curve defined over Q given by the Weierstrass normal form

$$E\colon y^2 = x^3 + ax + b, \qquad \Delta = -16(4a^3 + 27b^2) \neq 0,$$

with $a, b \in Z$. Assume that E has CM by an order in $K = Q(\sqrt{-d})$, an imaginary quadratic extension of Q, and a rational point of infinite order. By making a suitable transformation of the curve, we can assume without loss that our point of infinite order has integral coordinates. This is not essential but makes the subsequent discussion free from the annoying exclusion of a finite set of primes that do not necessarily come from primes for which E has bad reduction.

For any prime p and $(p, 6\Delta) = 1$, it makes sense to consider E as an elliptic curve over $\bar{F}_p$. If $E(F_p)$ is the group of F_p-rational points, then

$$\#E(F_p) = p + 1 - a_p, \qquad |a_p| \leq 2\sqrt{p}.$$

Also, as E is a CM curve, $a_p = 0$ roughly half the time, specifically according to

$$\begin{cases} \text{if } p \text{ is inert in } K, \text{ then } a_p = 0, \\ \text{if } p \text{ is split in } K, \text{ then } a_p = \operatorname{tr}(u\pi_p). \end{cases}$$

Here $\pi_p \bar{\pi}_p = p$, and u is one of the finitely many units in K.

We would like to view the fact that $|E(F_p)| = p+1$ whenever p is inert as analogous to the criterion used in the Fermat test that the order of the multiplicative subgroup of F_p is $p-1$. Since Z/nZ is not a field for composite n, it is more convenient to use the division polynomials. Let p be an inert prime, $(p, 6\Delta) = 1$. Then $\#E(F_p) = p+1$, and

$$\psi_{p+1}(P) \equiv 0 \pmod{p} \qquad \text{for any } P \in E(Z). \tag{3.1}$$

This calculation can be carried out for any n, prime or not. Accordingly, Gordon [6] fixes a point $P \in Z^2$ in $E(Q)$ of infinite order and tests:

Given n with $(n, 6\Delta) = 1$ and $\left(\frac{-d}{n}\right) = -1$, check whether or not

$$\psi_{n+1}(P) \equiv 0 \pmod{n}. \tag{3.2}$$

If so, and n is composite, we call n an elliptic pseudoprime (epsp).

So, one has a primality test that is analogous to the Fermat test in classical number theory. An obvious generalization is to test a given n with more than one point. Let us fix $P_1, \dots, P_r$, independent points of infinite order, and test for a given n as in (3.2) with each of these points. As before, we may assume, without loss of generality, that the points are integral by passing to an isomorphic curve via a suitable transformation. False witnesses to this test may be called generalized elliptic pseudoprimes.

One could generalize the test and define analogously strong elliptic pseudoprimes, or Euler elliptic pseudoprimes. The interested reader should look at Gordon [6] and some of the cited articles in his paper for tests involving non CM curves.

4. Upper Bounds. We fix E, an elliptic curve with CM and positive rank. Also suppose we have an independent set $\{P_1, \dots, P_r\}$ with $r \leq \operatorname{rank}(E) = r_E$. Let $\Gamma = \langle P_1, \dots, P_r \rangle$ and Γ_p be the subgroup of $E(F_p)$ generated by $\{P_1, \dots, P_r\}$.

Applying our test with E, we would like to know if it is effective at distinguishing primes from composites. For this to be the case, the number of false witnesses must be small in comparison to the number of primes. Accordingly, denote $N(x)$ to be the number of epsp not exceeding x. Gordon [6] has proved that

$$N(x) \ll \frac{x \log\log x}{(\log x)^2},$$

assuming a suitable GRH. This gives a probabilistic primality test using elliptic curves, but only *conditionally*. We will establish *unconditionally*,

THEOREM 1. *There holds*

$$N(x) \ll \frac{x(\log\log x)^{7/2}}{(\log x)^{3/2}}.$$

For our generalization to higher rank ($r_E \geq 2$), we establish a stronger upper bound.

THEOREM 2. *If* $r \geq 2$ *then*

$$N_\Gamma(x) \ll xR(x)^{-c}$$

for some $c > 0$, *where*

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

This is analogous to the bound established by Erdös [3] for Fermat pseudoprimes to the base 2 (see (1.1)), and we expect that it can be strengthened to the bound of Pomerance (see (1.3)), though the generalization is not immediate.

Remark 4.1. The proofs of both theorems are similar in spirit to Erdös [3] and Gordon [7], but with additional complications due to the fact that for split primes p, $|E(F_p)| \neq p+1$. The removal of the GRH in Theorem 2 is accomplished via a key lemma regarding the order of Γ_p for split primes p which simplifies the harder part of the argument. Some difficulty is encountered because of the fact that Γ_p may not be cyclic for a given p. However, this difficulty arises in the easier part of the analysis. In the rank 1 case this latter difficulty is not encountered. Nevertheless, the harder part of the argument is simplified to a narrow range by the use of the lemma.

Higher Rank Case: *Preliminary Lemmas.* Keeping the notation established so far, we will need

LEMMA 1. *The number of primes p for which $|\Gamma_p| < y$ is $O(y^{1+2/r})$.*

Proof. The result is proved using the canonical height pairing of Néron and Tate, and a result counting the number of lattice points contained in a particular r-dimensional ellipsoid. (See Gupta and Ram Murty [8] for a proof of this result.) □

In a similar fashion, Gupta and Ram Murty [8] prove what will be our key tool for estimation:

LEMMA 2. *The number of primes p for which $|\Gamma_p| < y$ and p splits in K is $O(y^{1+1/r})$.*

As in the Erdös paper [3], establishing the upper bound for Fermat psp in (1.1), we will need the following estimate adapted by Erdös [3] from the work of de Bruijn [2] on the number of $n \leq x$ composed of primes $p > y$.

LEMMA 3. *Let $N(p_1, \dots, p_k)$ denote the number of $n \leq x$ composed of primes from the set $\{p_1, \dots, p_k\}$ of k distinct primes. Put $k^u = x$. Then, for $u < \log x / \log\log x$, i.e., $k > \log x$,*

$$N(p_1, \dots, p_k) < x \exp(-cu \log u)$$

for some $c > 0$.

Proof. See Erdös[3] and de Bruijn [2]. □

LEMMA 4. *We may write $\Gamma_p = \Gamma_p^* \times U_p$ with Γ_p^* cyclic, and, if $b \mid |U_p|$, then $b \mid |\Gamma_p^*|$.*

Proof. The first part is clear since Γ_p is a finite abelian group. Being so, S_q, the q-Sylow subgroup of Γ_p, is unique and $\Gamma_p = \prod_{q \| \Gamma_p|} S_q$. Writing

$$S_q = C_{q^{n_1}} \times \cdots \times C_{q^{n_k}}, \qquad n_1 \geq \ldots \geq n_k \geq 0,$$

where $C_{q^{n_i}}$ is cyclic of order q^{n_i} (not necessarily unique), we note that $n_1 \geq \cdots \geq n_k \geq 0$ are uniquely determined. Moreover, $k \leq 2$, as the group of q^{n_1} division points of E over $\bar{F}_p$ is either cyclic or a product of 2 cyclic groups. The lemma follows by setting

$$\Gamma_p^* = \prod_{q||\Gamma_p|} C_{q^{n_1}}, \qquad U_p = \prod_{q||\Gamma_p|} C_{q^{n_2}}. \quad \square$$

We shall say that a group is of type (b, b) (or more briefly, a (b, b) group) if it is isomorphic to

$$Z/bZ \times Z/bZ.$$

COROLLARY 1. *$E(F_p)$ is cyclic if and only if $E(F_p)$ does not contain a (b, b) group for every b.*

COROLLARY 2. *For x sufficiently large,*

(i) *If $|\Gamma_p| \geq R(x)$ then $|\Gamma_p^*| \geq \sqrt{R(x)}$.*

(ii) *If $|\Gamma_p| > x^{1-\delta}$ for some $\delta > 0$, and $|U_p| < R(x)$, then $|\Gamma_p^*| > x^{1-\delta'}$ for any $\delta' > \delta$.*

Proof. (i) By Lemma 4, $|\Gamma_p| = |\Gamma_p^*||U_p| \leq |\Gamma_p^*|^2$, from which the result follows.
(ii)This follows from the fact that $R(x) \ll x^{\varepsilon}$ for any $\varepsilon > 0$. $\square$

Lemma 4 suggests the need to develop tools to estimate the number of primes p for which $E(F_p)$ contains a (b, b) group, b fixed.

LEMMA 5. *$E(F_p)$ contains a (b, b) group, $b \neq p$, if and only if p splits completely in $Q(E[b])$. (Here, $E[b]$ consists of the b-division points of $E(\overline{Q})$, and $Q(E[b])$ is the field obtained by adjoining the x and y coordinates of points $P \in E[b]$ to Q.)*

Proof. See Ram Murty [11]. $\square$

Let K be any number field. The ray class field belonging to an ideal $\mathscr{Q}$ is an abelian extension L of K such that the set of prime ideals of K which split completely in L are precisely those ideals lying in the unit class of the $\mathscr{Q}$ ideal class group (i.e., those prime ideals which are principal and generated by an element $\alpha \equiv 1 \pmod{q}$).

It is well known for elliptic curves with CM that $K(E[b])/K$ contains K_b, the ray class field belonging to bO_K, where $K = Q(\sqrt{-d})$ [10].

LEMMA 6. *Let E be an elliptic curve over Q with CM by an order O in K. There is an ideal f, depending only on E, such that*

$$K_m \subset L_m \subset K_{fm},$$

where K_m, K_{fm} are the ray class fields belonging to m and fm, respectively, and $L_m = K(E[m])$.

Proof. See Ram Murty [11]. $\square$

Coming back down to Q, we have

LEMMA 7. *$K(E[m]) = Q(E[m])$ for any $m > 2$ ($K = Q(\sqrt{-D})$).*

Proof. Clearly, it is enough to show that $K \subset Q(E[m])$. Let $\tau \in \mathrm{Gal}\,(\bar{Q}/Q)$ fixing $Q(E[m])$. Suppose that τ does not, however, fix K. Then τ restricted to K is complex conjugation. Let $\phi_\lambda \in \mathrm{End}(E)$ be multiplication by λ. Then $\mathrm{Gal}\,(\bar{Q}/Q)$

acts on End(E) as follows: for $\sigma \in \mathrm{Gal}\left(\bar{Q}/Q\right)$, $\sigma\phi_\lambda = \phi_{\sigma(\lambda)}$. Thus, $\tau\phi_\lambda = \phi_{\bar{\lambda}}$. Let $x \in E[m]$; then $\phi_\lambda(x) \in E[m]$, since

$$m(\lambda x) = \lambda(mx) = 0,$$

and therefore $\tau(\phi_\lambda(x)) = \phi_\lambda(x)$ since τ fixes $E[m]$. On the other hand, $\phi_\lambda(x) = \phi_{\bar{\lambda}}(x)$, hence

$$(\phi_\lambda - \phi_{\bar{\lambda}})(x) = \phi_{\lambda - \bar{\lambda}}(x) = 0.$$

Thus, $\lambda \equiv \bar{\lambda} \pmod{mO_K}$. Let f denote the conductor of O; then as every order O of K is of the form $Z + fO_K$, the above congruence holds in particular for $\lambda = f\sqrt{-D}$, whence

$$2f\sqrt{-D} \equiv 0 \pmod{mO},$$

in which case $2f\sqrt{-D} = mbf\sqrt{-D}$ for some b. We conclude that $mb = 2$, so $m \mid 2$.

As long as $m > 2$, then τ acts trivially on K, so $Q(E[m]) \supset K$ as desired, whence $Q(E[m]) = K(E[m])$. □

Finally, by very elementary means, one proves the useful estimate

LEMMA 8. *The number of $\alpha \in O_K$, $\alpha \notin Z$, and $N\alpha \leq x$, such that $\alpha \equiv 1 \pmod{mO_K}$ is*

$$\ll \frac{x}{m^2} + \frac{\sqrt{x}}{m}.$$

(Here $N\alpha$ is the norm of α.)

Proof. Let $1, \omega$ be an integral basis of O_K. Then, $\alpha = a + b\omega$ for some $a, b \in Z$. Since $\alpha \equiv 1 \pmod{mO_K}$, $a - 1 = mc$ and $b = md$ for some $c, d \in Z$. As $N(\alpha) \leq x$, $a^2 + Db^2 \leq x$ or $(a + b/2)^2 + Db^2/4 \leq x$, depending on the congruence condition satisfied by $D \pmod 4$. We deal with the former case, the latter one being similar. Thus, $|a| \leq \sqrt{x}$. Now, $a \equiv 1 \pmod m$ implies that there are

$$2\frac{\sqrt{x}}{m} + 1$$

possibilities for a. The number of possibilities for b is $\leq 2\sqrt{x}/m$ as $b \neq 0$. Combining these estimates gives the final result. □

We are now ready to prove Theorem 2.

5. Proof of Theorem 2. Keeping the notation of the preliminary lemmas, let $R(x) = \exp(\sqrt{\log x \log\log x})$. Let us write any epsp $n \leq x$ as $n = sL$ where

$$\begin{cases} p \mid s \Leftrightarrow |\Gamma_p| \leq R(x), \\ p \mid L \Leftrightarrow |\Gamma_p| > R(x). \end{cases}$$

We will split the epsp into four classes:

(1) $L = 1$.
(2) There is an inert prime $p \mid L$.
(3) There is a split prime $p \mid L$ with $|\Gamma_p| < x^{1-\delta}$.
(4) $L > 1$ and for all $p \mid L$, p splits in K and $|\Gamma_p| \geq x^{1-\delta}$.

The constant $\delta > 0$ will be chosen later.

We should remark that the above list exhausts all the cases, as only finitely many primes p ramify in K. Thus, there are only finitely many corresponding Γ_p. For large x, therefore, all such Γ_p will have $|\Gamma_p| \le R(x)$, hence L will then contain only (possibly) split or inert factors.

By Lemma 1 any epsp in class 1 will have at most $R(x)^{1+2/r}$ prime divisors. Applying Lemma 3 with $k = R(x)^{1+2/r}$, so that

$$u = \frac{r}{r+2}\left(\frac{\log x}{\log\log x}\right)^{1/2},$$

we find that the number of epsp in class 1 is at most

$$\frac{x}{R(x)^{c_1}} \quad \text{for some } c_1 > 0. \tag{5.1}$$

If n is an epsp with $p \mid n$ then by Lemma 4, there is an element of Γ_p of order $|\Gamma_p^*|$. Hence,

$$\begin{cases} n \equiv 0 \pmod{p}, \\ n \equiv -1 \pmod{|\Gamma_p^*|}. \end{cases} \tag{5.2}$$

Let us note that (5.2) implies that $(p, |\Gamma_p^*|) = 1$. So, by the Chinese remainder theorem, the number of such n satisfying (5.2) is at most

$$1 + \frac{x}{p|\Gamma_p^*|}. \tag{5.3}$$

However, in class 2, n has an inert prime divisor p which itself satisfies the congruences in (5.2), because $|\Gamma_p| | p+1$. We remove the prime from our count as we are enumerating composite numbers which pass the pseudoprime test. Therefore, we get at most

$$\frac{x}{p|\Gamma_p^*|}$$

composite solutions, since $(p, |\Gamma_p|) = 1$. The number of epsp in class 2 therefore does not exceed

$$\begin{aligned} \sum_{\substack{p<x \\ |\Gamma_p|>R(x)}} \frac{x}{p|\Gamma_p^*|} &\ll \sum_{\substack{p<x \\ |\Gamma_p^*|\ge\sqrt{R(x)}}} \frac{x}{p|\Gamma_p^*|} \ll \frac{x}{\sqrt{R(x)}} \sum_{p<x} \frac{1}{p} \\ &\ll \frac{x\log\log x}{\sqrt{R(x)}} \ll \frac{x}{R(x)^{1/4}}, \end{aligned} \tag{5.4}$$

where the first inequality is from Corollary 2(i) to Lemma 4.

If n is in class 3, let

$$p \mid n, \quad p \text{ split in } K, \quad R(x) < |\Gamma_p| < x^{1-\delta}. \tag{5.5}$$

Then using (5.3), the number of epsp in class 3 is at most

$$\sum_{p<x}{}' \left(1 + \frac{x}{p|\Gamma_p^*|}\right) \ll \sum{}' 1 + \sum{}' \frac{x}{p|\Gamma_p^*|},$$

where the $\sum'$ indicates the range of summation in (5.5).

The second sum may be estimated as before in (5.4), using Corollary 2 of Lemma 4,

$$\sum_{p<x}{}' \frac{x}{p|\Gamma_p^*|} \ll \frac{x}{R(x)^{1/4}}.$$

For the first sum, we use Lemma 2. The number of primes p which split in K for which $|\Gamma_p| < x^{1-\delta}$ is $\ll x^{(1-\delta)(1+1/r)}$. Hence

$$\sum{}' 1 \ll x^{(1-\delta)(1+1/r)} \ll x^{1-3\eta/2}, \tag{5.6}$$

by writing $\delta = 1/3 + \eta$, and we will choose $\eta > 0$ later. (Since $r \geq 2$, any $\delta > 1/3$ works.)

If n is in class 4, then every p dividing n with $|\Gamma_p| > R(x)$ splits in K and has $|\Gamma_p| > x^{1-\delta}$. Using Lemma 4, Corollary 2(i), let us consider two subclasses:

(a) The largest (b, b) group $\subset \Gamma_p$ (if any) has $b \leq \sqrt{R(x)}$.

(b) The largest (b, b) group $\subset \Gamma_p$ has $b > \sqrt{R(x)}$.

In (a), $|\Gamma_p^*| > x^{1-\delta'}$ for any $\delta' > \delta$ by Corollary 2(ii) of Lemma 4. As in (5.4), the number of epsp in this class is at most

$$\sum_{\substack{|\Gamma_p^*|>x^{1-\delta'} \\ p \text{ split } \leq x}} \left(1 + \frac{x}{p|\Gamma_p^*|}\right) \ll \sum{}'' 1 + \sum{}'' \frac{x}{p|\Gamma_p^*|}, \tag{5.7}$$

where the double dash indicates the specified condition on Γ_p^* and p.

The second sum is

$$\sum{}'' \frac{x}{p|\Gamma_p^*|} \ll \frac{x}{R(x)^{1/4}} \tag{5.8}$$

as usual. (In fact $\ll x^{1-\delta'}$.)

In the first sum, we may assume that $p > x^{1-\varepsilon}$, where $\varepsilon > 0$ is to be chosen later. This is because $p \leq x^{1-\varepsilon}$ implies

$$\sum_{p \leq x^{1-\varepsilon}}{}'' 1 \ll x^{1-\varepsilon}. \tag{5.9}$$

But now, for $p > x^{1-\varepsilon}$, a simple argument shows that the corresponding sum is void for large x. Indeed,

$$\begin{cases} p + 1 - a_p \equiv 0 \pmod{|\Gamma_p^*|}, \\ n + 1 \equiv 0 \pmod{|\Gamma_p^*|}, \\ p \mid n, \quad n = mp, \end{cases}$$

thus

$$mp + 1 \equiv m(a_p - 1) + 1 \equiv 0 \pmod{|\Gamma_p^*|},$$

so $m(a_p - 1) + 1 > |\Gamma_p^*| > x^{1-\delta'}$, whence $m \gg x^{1/2-\delta'}$ as $|a_p| \leq 2\sqrt{p}$. But then,

$$n = mp \gg x^{1/2-\delta'} x^{1-\varepsilon} = x^{3/2-\delta'-\varepsilon}. \tag{5.10}$$

Recall that we may choose η and $\delta' > 0$ freely so that $\delta' > \delta = 1/3+\eta$. Choosing $\varepsilon > 0$ so that $\delta' + \varepsilon < 1/2$, we find from (5.10) that $n > x$, which is a contradiction. It follows that for large x,

$$\sum_{p > x^{1-\varepsilon}}{}'' 1 = 0. \tag{5.11}$$

Combining (5.8), (5.9), and (5.11), we conclude that the number of epsp in class 4(a) is $\ll x^{1-\delta'}$.

(In the rank 1 case we would be forced to choose $\delta > 1/2$, say $\delta = 1/2 + \eta$, in (5.6). This would make it impossible to choose $\delta' > \delta$ and $\varepsilon > 0$ so that $\delta' + \varepsilon < 1/2$, as was required in (5.10).)

Finally, suppose that n is in class 4(b). Then any prime divisor p with $|\Gamma_p| > R(x)$ splits in K and has $|\Gamma_p| > x^{1-\delta}$. Moreover, Γ_p contains a (b, b) group with $b > \sqrt{R(x)}$. By Lemma 5, p splits completely in $Q(E[b])$. By Lemma 7, p splits completely in $K(E[b])$. By Lemma 6, $K(E[b]) \supseteq K_b$. Hence, if p splits completely in $K(E[b])$, it splits completely in K_b. That is,

$$p = \pi_p \bar{\pi}_p, \qquad \pi_p \equiv 1 \pmod{bO_K}.$$

By Lemma 8, the number of $\alpha \notin Z$, $\alpha \in O_K$ for which $\alpha \equiv 1 \pmod{b}$ is $\ll x/b^2 + \sqrt{x}/b$.

Therefore, the number of epsp in 4(b) is at most

$$\sum{}' \left(1 + \frac{x}{p|\Gamma_p^*|}\right) \ll \sum{}' 1 + \sum{}' \frac{x}{p|\Gamma_p^*|} \ll \sum{}' 1 + \frac{x}{R(x)^{1/4}}$$

as usual, where $\sum'$ indicates that the range of summation is

$$p < x,\ p \text{ split},\ |\Gamma_p^*| > x^{1-\delta'},\ \text{and } \Gamma_p \supset (b,b) \text{ group},\ b > \sqrt{R(x)}.$$

But the first sum is

$$\ll \sum_{\sqrt{R(x)} \le b \le 2x} \left(\frac{x}{b^2} + \frac{\sqrt{x}}{b}\right),$$

by the remarks above. This is easily estimated to be

$$\ll \frac{x}{\sqrt{R(x)}} + \sqrt{x} \log x. \tag{5.12}$$

Putting all the estimates (5.1), (5.4), (5.6), (5.9), (5.11) and (5.12) together, we find that the number of epsp $\le x$ is at most $xR(x)^{-c}$ for some $c > 0$ as desired. □

6. Rank 1 Case. During the proof of Theorem 2 we remarked that Lemma 2 cannot be applied to as large a range for $|\Gamma_p|$. Indeed, we were able to estimate the number of elliptic pseudoprimes with a split prime factor p such that $R(x) < |\Gamma_p| < x^{1-\delta}$, provided $\delta > 1/3$. The same argument carries over to the rank 1 case if $\delta < 1/2$. The analysis used in (5.10) however, does not carry over and a more delicate analysis is needed.

We will need the following estimate:

LEMMA 9. *There holds*

$$\sum_{y < \delta < z} \frac{1}{\delta} \ll \frac{(\log\log x)^{3/2}}{\sqrt{\log x}},$$

where we assume that any $p|\delta$ *satisfying* $p > \log^2 x$ *splits in* K, *and* $y = x^{1/2} \log^{-A} x$ *and* $z = x^{1/2} \log^{A} x$ *for some fixed* $A > 0$.

Proof. Since $K = Q(\sqrt{-d})$, the density of primes which split in K is $1/2$. Therefore, by standard analytic number theory, we have that as $v \to \infty$,

$$\prod_{\substack{q<v \\ q \text{ inert in } K}} \left(1 - \frac{1}{q}\right) \sim \frac{C_K}{\sqrt{\log v}},$$

where C_K is a constant depending only on K. Using Brun's sieve [9], we estimate the number $C(x;w)$ of $\delta \le x$, all of whose prime factors $> w$ split in K. Then, $C(x;w)$ is bounded by

$$x \prod_{\substack{w<q<x^{1/3} \\ q \text{ is inert in } K}} \left(1 - \frac{1}{q}\right) \ll \frac{x\sqrt{\log w}}{\sqrt{\log x}}.$$

(See Erdös [4] or Halberstam and Richert[9].)

By partial summation,

$$\sum_{y<\delta<z} \frac{1}{\delta} \ll \frac{C(z;w)}{z} + \int_y^z \frac{C(t;w)}{t^2} dt,$$

where the summation over δ is as stated in the lemma. With $w = \log^2 x$, and by our choices of y and z, the sum is easily seen to be

$$\ll \frac{(\log\log x)^{3/2}}{\sqrt{\log x}}. \quad \square$$

Proof of Theorem 1. To simplify the notation, let e_p denote the order of P (mod p).

Write as before any pseudoprime $n \le x$ as $n = sL$, where

$$\begin{cases} p \mid s \Leftrightarrow e_p \le R(x), \\ p \mid L \Leftrightarrow e_p > R(x). \end{cases}$$

Split the pseudoprimes into five classes:

(1) $L = 1$.
(2) There is an inert prime $p \mid L$.
(3) There is a split prime $p \mid L$ with $e_p \le \sqrt{x}\log^{-A} x$.
(4) There is a split prime $p \mid L$ with $e_p \ge \sqrt{x}\log^{A} x$.
(5) $L > 1$ and all $p \mid L$ are split and $\sqrt{x}\log^{-A} x < e_p < \sqrt{x}\log^{A} x$.

Class (1) is identical to the higher-rank situation.

Lemma 1 provides at most $R(x)^3$ prime divisors for n in this class, and Lemma 3 implies at most

$$\frac{x}{R(x)^{c_1}} \tag{6.0}$$

such n, for some $c_1 > 0$.

Class (2) is as before:

If n is a pseudoprime and $p \mid n$, then

$$\begin{cases} n \equiv 0 \pmod{p}, \\ n + 1 \equiv 0 \pmod{e_p}, \\ (p, e_p) = 1, \end{cases} \tag{6.1}$$

and the number of solutions to (6.1) is at most

$$\frac{x}{pe_p} + 1. \tag{6.2}$$

But when n is in class (2), there is a p inert dividing n which is, itself, a solution of (6.1). Hence the number of composite solutions to (6.1) is at most x/pe_p. Therefore the number of pseudoprimes in this class does not exceed

$$\sum_{\substack{p<x \\ e_p>R(x)}} \frac{x}{pe_p} \ll xR(x)^{-1/2}. \tag{6.3}$$

These two classes are therefore treated as in Gordon [6].

For class (3), we estimate

$$\sum{}' \left(1 + \frac{x}{pe_p}\right) \ll \sum{}' 1 + \sum{}' \frac{x}{pe_p},$$

where $\sum'$ means the range of summation

$$p < x, \quad p \text{ split in } K, \text{ and } R(x) < e_p \leq \sqrt{x} \log^{-A} x.$$

The second sum is

$$\ll \frac{x}{R(x)^{1/2}},$$

as in (6.3), and the first sum is estimated using Lemma 2, so that

$$\sum{}' 1 \ll \frac{x}{\log^{2A} x}.$$

Therefore, the number of pseudoprimes in this class is at most

$$\frac{x}{\log^{2A} x} + \frac{x}{R(x)^{1/2}}. \tag{6.4}$$

For class (4), $\Gamma_p = \langle P \rangle$ is cyclic, and so we can proceed as in class 4(a) in the proof of the higher-rank case. The number of pseudoprimes in this class is at most

$$\sum{}' \left(1 + \frac{x}{pe_p}\right) \ll \sum{}' 1 + \sum{}' \frac{x}{pe_p} \ll \sum{}' 1 + \frac{x}{R(x)^{1/2}},$$

as in (6.3), where now $\sum'$ indicates a range of summation

$$p < x, \quad p \text{ split in } K, \text{ and } e_p > \sqrt{x} \log^{A} x.$$

We may assume that $p > 3x/\log^A x$, since

$$\sum_{p \leq 3x \log^{-A} x}{}' 1 \ll \frac{x}{\log^A x}. \tag{6.5}$$

But now for $p > 3x/\log^A x$ we find that $\sum' = 0$, since (6.1) implies that $n = sp$, and

$$s(a_p - 1) + 1 > e_p > \sqrt{x} \log^A x,$$

so that $s \geq \frac{1}{2} \log^A x$ using $|a_p| \leq 2\sqrt{p}$. Therefore $n = sp \geq 3x/2$, which is a contradiction.

Thus the number of pseudoprimes in class (4) is at most

$$\frac{x}{\log^A x} + \frac{x}{R(x)^{1/2}}. \tag{6.6}$$

For n in class (5) we change our strategy a little bit.

Let n be a pseudoprime in this class, with $p \mid L$. Again, we may assume that $p > x \log^{-A} x$. Let

$$S = \{p \leq x \colon \sqrt{x} \log^{-A} x < e_p < \sqrt{x} \log^{A} x\};$$

then $p \in S$ and is split in K. As $e_p \mid n+1$, we may write $n+1$ as a product of factors uv, each approximately $\sqrt{x}$, i.e., up to powers of log. We note that for p split,

$$e_p \mid p + 1 - a_p = (\pi_p - 1)(\bar{\pi}_p - 1)$$

for some factorization of p in O_K. Therefore, if q is inert and $q \mid e_p$, then $q \mid \pi_p - 1$ (and $\bar{\pi}_p - 1$). But then, by Lemma 8, the number of primes $p = \alpha\bar{\alpha}$ such that $\alpha \equiv 1 \pmod q$ is

$$\ll \frac{\sqrt{x}}{q}\left(1 + \frac{\sqrt{x}}{q}\right).$$

If $q > \log^2 x$, then we obtain an estimate of

$$\ll \frac{x}{\log^2 x} + \sqrt{x} \log x$$

such primes p.

Accordingly, we consider two subclasses:

(a) There exists an inert $q > \log^2 x$ dividing e_p, or

(b) If $q > \log^2 x$, and divides e_p, then q splits in K.

In (a), the above remarks show that the number of elliptic pseudoprimes in this case is

$$\frac{x}{\log^2 x} + \sqrt{x} \log x. \tag{6.7}$$

In (b), let

$$\begin{aligned} N_p(x) &= \#\{n : \ n \text{ is an epsp and } p \mid n\}, \\ d'(n; x) &= \#\{\delta : \ \delta \mid n, \ \sqrt{x} \log^{-A} x < \delta < \sqrt{x} \log^{A} x, \\ &\qquad \text{and if } p \mid \delta, \text{ and } p > \log^2 x, \text{ then } p \text{ splits in } K\}. \end{aligned}$$

Note that if n is in class (b), $d'(n+1; x) \geq 1$ because e_p is a divisor of $n+1$ satisfying (b). Therefore, the number of pseudoprimes in this class is at most

$$\sum_{p}{}' N_p(x) = \sum_{p}{}' \sum_{\substack{n = sp \\ e_p \mid n+1}} 1 \leq \sum_{\substack{p > x \log^{-A} x \\ s \leq \log^A x}}{}' d'(sp + 1; x), \tag{6.8}$$

by the definitions above, where $\sum'$ indicates the range of summation

$$p \text{ splits, and } \sqrt{x} \log^{-A} x \leq e_p \leq \sqrt{x} \log^{A} x, \textit{ and } \text{the hypothesis (b).}$$

Interchanging the order of summation, we get

$$\leq \sum_{p,s}{}' \sum_{\delta \mid sp+1} 1 = \sum_{\delta}{}' \sum_{s \leq \log^A x} \sum_{sp \equiv -1 \pmod{\delta}} 1, \tag{6.9}$$

where in the sum, δ satisfies

$$\sqrt{x}\log^{-A} x < \delta < \sqrt{x}\log^{A} x$$

and all prime factors of δ greater than $\log^2 x$ are split in K. If ϕ denotes the Euler function, the innermost sum is, by the Brun-Titchmarsh theorem [9],

$$\ll \frac{x/s}{\phi(\delta)\log(x/s\delta)} \ll \frac{x}{s\phi(\delta)\log x},$$

applied to

$$\#p \leq x, \qquad sp+1 = \delta t \leq x, \quad \text{so } p \leq x/s.$$

Thus, the number of elliptic pseudoprimes is

$$\ll {\sum_{\delta}}' \sum_{s \leq \log^A x} \frac{x}{s\phi(\delta)\log x} \ll {\sum_{\delta}}' \frac{x \log\log x}{\phi(\delta)\log x}. \tag{6.10}$$

Since $\phi(\delta) \gg \delta/\log\log\delta$, we obtain that this is

$$\ll {\sum_{\delta}}' \frac{x(\log\log x)^2}{\delta \log x}.$$

But then, applying Lemma 9 to the above sum, and noting that $\sqrt{x}\log^{-A} x < \delta < \sqrt{x}\log^{A} x$, we find that the number of pseudoprimes in this class is

$$\ll \frac{x(\log\log x)^{7/2}}{\log^{3/2} x}. \tag{6.11}$$

Finally choosing $A > 2$, we see that our estimates, all together, give

$$\#\{\text{epsp} \leq x\} \ll \frac{x(\log\log x)^{7/2}}{\log^{3/2} x},$$

as desired. □

A slightly more careful analysis might eliminate a part of the log log factor in the numerator.

Department of Mathematics and Statistics
McGill University
Montreal, Quebec, Canada
E-mail for M. Ram Murty: mt88@mcgilla.bitnet

1. J. W. S. CASSELS, "Arithmetic on an elliptic curve," *Proc. London Math. Soc.*, v. 14, 1964, pp. 259–296.

2. N. G. DE BRUIJN, "On the number of positive integers $\leq x$ and free of prime factors $> y$," *Indag. Math.*, v. 13, 1951, pp. 50–60.

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

4. P. ERDÖS, "On the converse of Fermat's theorem," *Amer. Math. Monthly*, v. 56, 1949, pp. 623–624.

5. P. ERDÖS & CARL POMERANCE, "On the number of false witnesses for a composite number," *Math. Comp.*, v. 46, 1986, pp. 259–279.

6. D. M. GORDON, "On the number of elliptic pseudoprimes," *Math. Comp.*, v. 52, 1989, pp. 231–245.

7. D. M. GORDON, Private communication.

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

9. H. HALBERTSTAM & H. E. RICHERT, *Sieve Methods*, Academic Press, London, 1974.

10. S. LANG, *Elliptic Functions*, Addison-Wesley, Reading, Mass., 1973.

11. M. RAM MURTY, "On Artin's conjecture," *J. Number Theory*, v. 16, 1983, pp. 147–168.

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

13. J. H. SILVERMAN, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.

14. J. T. TATE, "The arithmetic of elliptic curves," *Invent. Math.*, v. 23, 1974, pp. 171–206.