Extending Lenstra's Primality Test to CM Elliptic Curves and a new Quasi-Quadratic Las Vegas Algorithm for Primality

Tejas Rao

December 2022

Abstract

For an elliptic curve with CM by K defined over its Hilbert class field, E/H, we extend Lenstra's finite fields test to generators of norms of certain ideals in $\mathcal{O}_H$, yielding a sufficient $\widetilde{O}(\log^3 N)$ primality test and partially answering an open question of Lemmermeyer. Specializing this test to a smaller class of generators of norms of ideals, we give a Las Vegas test for primality with average runtime $\widetilde{O}(\log^2 N)$, that further certifies primality in $\widetilde{O}(\log^2 N)$ for nearly all choices of input parameters. The integers tested were not previously amenable to quasi-quadratic heuristic primality cerftification.

1 Preliminaries

Fast primality testing of a rational integer N relies on a theme of Lucas, wherein a finite group is constructed so (provably) large that N must be prime. Pomerance outlines the classical methods arising from this theme [3]. The binary modular exponentiation central to this Lucasian theme runs in $\widetilde{O}(\log^2 N)$, providing a hypothetical lower bound to all primality testing barring a new theme. Pomerance proved that this hypothetical minimum bound is met: there exist $\widetilde{O}(\log^2 N)$ certifications of primality for every rational prime [3]. *Finding* these certifications, i.e. testing for primality, is another story. The fastest classical test relies on a known factorization of $N^k - 1$ for some fixed small $k \in \mathbb{N}$, and runs in heuristic $\widetilde{O}(\log^3 N)$ time:

Theorem 1.1 (Lenstra's Finite Fields Test, [3, 4])**.** *Let N, k positive integers, $N > 1$ and $f \in (\mathbb{Z}/N\mathbb{Z})[x]$ monic of degree k. Suppose that $F | N^k - 1$, $F > \sqrt{N}$, and F has a known prime factorization. If $\exists g \in (\mathbb{Z}/N\mathbb{Z})[x]$ such that in*

$(\mathbb{Z}/N\mathbb{Z})[x]/(f)$,

(1) $g^F = 1$,

(2) $\gcd(g^{\frac{F}{q}} - 1, f) = 1$, *for each prime* $q|F$,

(3) each elementary symmetric polynomial in $g^{N^j}, 0 \leq j \leq k-1$ *has coefficients in* $\mathbb{Z}/N\mathbb{Z}$,

and if none of the residues $N^j \mod F$, $0 \leq j \leq k-1$, *are proper factors of* N, *then* N *is prime.*

Similar to Pocklington's criterion, multiple bases g may be chosen [4]. The algorithm runs in heuristic $\widetilde{O}(k^2 \log^3 N)$, and tests based on it are referred to as cyclotomic primality tests [13]. The runtime of this algorithm is deterministically $\widetilde{O}(\log^2 N)$ if k is small and fixed, the number of prime powers of F is polynomial in $\log\log N$, and a suitable g (or multiple bases) is known; it remains heuristic $\widetilde{O}(\log^2 N)$ time even if the bases g are not known beforehand. This is the hypothetical minimum runtime of Lucasian tests, and an algorithm having such (at least heuristic) runtime will henceforth be referred to as an *efficient primality test*.

Beyond classical primality testing, the theory of Ellipitic Curve Primality Proving (ECPP) has been developed by such figues as Goldwasser, Kilian, Atkin, and Morain [1, 2]. In the seminal Elliptic Curve Primality Proving paper by Atkin and Morain [2], the theory of complex multiplication (CM) is used to determine the orders of certain elliptic curves and test for primality of any positive integer N. An asymptotically-fast version due to Shallit runs in heuristic $\widetilde{O}(\log^4 N)$ time and stands as our fastest general algorithm in practice [7]. More recently, Milhailescu proposed a variant general primality test running one round of cyclotomic primality testing, followed by a round of ECPP, running in heuristic $\widetilde{O}(\log^3 N)$ time, which would stand as the fastest general algorithm [14]. Importantly, it does not reduce to an *efficient primality test* when the number of prime power factors of F is polynomial in $\log\log N$. General testing is not yet $\widetilde{O}(\log^2 N)$, and thus there has been work done to determine $\widetilde{O}(\log^2 N)$ testing utilizing elliptic curves, expanding the class of rational integers amenable to *efficient primality tests* [8]. Specifically, Abatzoglou, Sutherland, Wong, and Silverberg use CM elliptic curves to provide a framework for deterministic efficient primality testing for certain sequences of integers not amenable to classical testing [8, 9]. A recent preprint in the same vein proposes an extension of the results to characteristic 3 [18].

In the open problems section of his celebrated work Reciprocity Laws: From Euler to Eisenstein [15], Lemmermeyer asks:

> Can Lenstra's Primality Test be generalized so as to include primality tests based on elliptic curves?

In this paper, we answer this question in the affirmative for certain inputs in the case of CM elliptic curves, producing an analogue heuristic $\widetilde{O}(k^2 \log^3 N)$

primality test that reduces to heuristic $\widetilde{O}(\log^2 N)$ when k and the number of certain prime power factors is small. To avoid precomputing the complex isogenies of the CM elliptic curve, we introduce another efficient primality test for a smaller class of numbers, this time which provides a certificate of primality of a prime p in one trial with probability $1 - 1/p^\alpha$ for some reasonably-sized α, and is a Las Vegas primality algorithm with average runtime $\widetilde{O}(\log^2 N)$ for certain new classes of integers not amenable to previous efficient primality tests.

2 Extending Lenstra's Criterion

2.1 Definitions

Throughout this paper, p, q refer to rational primes. Further, E/M refers to an elliptic curve defined over some number field M and $\mathcal{O}_M$ denotes the ring of integers of M. Let $h(M)$ denote the class number. For a Dedekind domain (e.g. the ring of integers of a number field) we adopt the definition $\gcd(\mathfrak{j}, \mathfrak{i}) = \mathfrak{j} + \mathfrak{i}$ for two ideals $\mathfrak{j}, \mathfrak{i}$. We note that there is no proper ideal containing both $\mathfrak{j}, \mathfrak{i}$ precisely when $\gcd(\mathfrak{j}, \mathfrak{i}) = (1)$. Further, let $N_{L/V}$ denote the field norm for a field extension L/V.

The number fields of interest for most of this paper are imaginary quadratic fields K with Hilbert class field H. We let E/H be an elliptic curve defined over $H \supset K$ with complex multiplication by the ring of integers $\mathcal{O}_K$ of K. We further let $\phi_{E,q}$ be the Frobenius endomorphism on the group $E(\overline{\mathbb{F}}_q)$ given by $\phi([x : y : z]) = [x^q : y^q : z^q]$. Further we will make the simplifying assumption that $K \neq \mathbb{Q}[\sqrt{-1}], \mathbb{Q}[\sqrt{-3}]$ so that the unit group of $\mathcal{O}_K$ is $\{\pm 1\}$, although it should be noted that much of the theory can be extended without much trouble to these cases.

Let $\mathfrak{N} \subset \mathcal{O}_H$ be an ideal such that $N_{H/K}(\mathfrak{N}) = \pi\mathcal{O}_K$ for some $\pi \in \mathcal{O}_K$. Also let $N \in \mathbb{N}$ be one of the non-negative integers such that $N\mathbb{Z} = N_{K/\mathbb{Q}}(\pi\mathcal{O}_K) = N_{H/\mathbb{Q}}(\mathfrak{N})$. We also consider prime ideals of $\mathcal{O}_H$, $\mathfrak{p}$, with $N_{H/K}(\mathfrak{N}) = \pi_p\mathcal{O}_K$ and $N_{H/\mathbb{Q}}(\mathfrak{p}) = p^j$ for a rational positive prime p.

Also let $f_k \in (\mathcal{O}_H/\mathfrak{N})[x]$ be a monic (over $\mathcal{O}_H/\mathfrak{N}$) polynomial of degree k given by $x^k - a$, where $a \in \mathcal{O}_H$ satisfies $\gcd((y^j - a)\mathcal{O}_H, \mathfrak{N}) = (1)$ for all $0 \leq j < k$. In particular, for each prime $\mathfrak{p}|\mathfrak{N}$, this reduces to a cyclic Galois extension with Galois group $G_\mathfrak{p}$ generated by the Frobenius $\sigma_\mathfrak{p} : x \mapsto x^{\operatorname{char} \mathcal{O}_H/\mathfrak{p}}$. For the set up above, if $\mathfrak{N}$ is prime and $N_{H/\mathbb{Q}}(\mathfrak{N}) = N$ is not a perfect power, then $x^N = \zeta_k x$ for some primitive k-th root of unity modulo $\mathfrak{N}$, $\zeta_k \in \mathcal{O}_H$. For general $\mathfrak{N}$, define the map $\sigma_{G_N,j}$ by $\sigma_{G_N,j}(\sum_{i=0}^{k-1} a_i x^i) = \sum_{i=0}^{k-1} a_i \zeta_{k,j}^i x^i$ for some *primitive* k-th root of unity $\zeta_{k,j}$.

Let $P = [x_0 : y_0 : z_0] \in E(\mathcal{O}_H)$. We write $P \mod \mathfrak{N}$ to denote the coordinate-wise reduction of P modulo $\mathfrak{N}$. Note that we have that $P \equiv O_E \mod \mathfrak{N} \Leftrightarrow z_0 \in \mathfrak{N}$. Following the convention of [8, 9], we say P is *strongly nonzero* modulo $\mathfrak{N}$ if $\gcd(z_0\mathcal{O}_H, \mathfrak{N}) = (1)$. In particular this implies $z_0\mathcal{O}_H$ and $\mathfrak{N}$ are relatively prime. In particular this implies that for each prime $\mathfrak{p}|\mathfrak{N}$, $P \not\equiv O_E \mod \mathfrak{p}$.

Now if $P = [x_0 : y_0 : z_0] = [x_0 : y_0 : \sum_{x=0}^{k-1} a_i x^i] \in E(\mathcal{O}_H[x]/(f_k))$, we note that

$$P \equiv O_E \mod \mathfrak{N} \Leftrightarrow z_0 \in \mathfrak{N} \Leftrightarrow a_i \in \mathfrak{N}, 0 \leq i \leq k-1$$

Thus we say P is *strongly non-zero* modulo $\mathfrak{N}$ if $\gcd(a_i\mathcal{O}_H, \mathfrak{N}) = (1)$ for $0 \leq i \leq k-1$. In particular this implies that $a_i \notin \mathfrak{p}$ for each prime $\mathfrak{p}|\mathfrak{N}$ and thus that $P \not\equiv O_E \mod \mathfrak{p}$.

Remark 2.1. If one wants to confirm $\gcd(a\mathcal{O}_H, \mathfrak{N}) = (1)$, simply show that $\gcd(N_{H/\mathbb{Q}}(a\mathcal{O}_H), N) = 1$.

2.2 Hecke Character Properties

Consider again E/H with CM by $\mathcal{O}_K$ ($K \subset H$). Again recall that throughout this paper $K \neq \mathbb{Q}[i], \mathbb{Q}[\sqrt{-3}]$. We adopt and specialize the following definition-lemma from [12, Prop. 4.1].

Lemma 2.2. *Let* $\psi : I(B) \to K^\times$ *denote the* Hecke Character *given as the unique character from the group of fractional ideals with support outside of primes* $\beta \in \mathcal{O}_H$ *where* E *has bad reduction satisfying:*

(1) $\psi(\mathfrak{p}) \in \mathcal{O}_K$*, and* $\psi(\mathfrak{p})$ *is a generator of* $N_{H/K}(\mathfrak{p})$
(2) $|E(\mathcal{O}_H/\mathfrak{p})| = N_{H/\mathbb{Q}}(\mathfrak{p}) + 1 - Tr_{K/\mathbb{Q}}(\psi(\mathfrak{p}))$

Proof. We must check that Proposition 4.1 specializes to this case when we take the order in K, $\mathcal{O} = \operatorname{End} E$, to be $\mathcal{O}_K$, and when we let $K \neq \mathbb{Q}[i], \mathbb{Q}[\sqrt{-3}]$. But this is precisely the content of [12, Lemma 2.6, Remark 2.7, Corollary 4.2]. Notice that conditions $(ii), (iii)$ of [12, Prop. 4.1] are trivially satisfied in this special case because $\mathcal{O} = \mathcal{O}_K$. □

In particular, $\psi(\mathfrak{p}) \in \mathcal{O}_K$ is the Frobenius endomorphism of E defined over $\mathcal{O}_H/\mathfrak{p}$. The above paper gives a method of calculating the Hecke character for certain primes $\mathfrak{p}$ in a method that is negligible in computational complexity compared to the runtime of the algorithm 3.3, as spelled out below in Definition 2.3, Lemma 2.4, and [12, Prop. 6.2]. In particular, we have that

$$\psi(\mathfrak{p}) = u\pi_p$$

We define the analogs $\left(\frac{a}{\mathfrak{N}}\right)$ of the Legendre symbol as in [[12, Def. 2.3]], except we all $\mathfrak{N}$ to be composite in the definition.

For some unit $u \in \mathcal{O}_K^\times$. Since we have removed $\mathbb{Q}[i], \mathbb{Q}[\sqrt{-d}]$, $u = \pm 1$. Let D be the discriminant of K. We make the following definition:

Definition 2.3. Suppose $E : y^2 = x^3 + ax + b$. Let τ be as in [12, Prop. 5.3]. Recall $\pi := N_{H/K}(\mathfrak{N})$. Let ϵ_τ be as in [12, Prop 6.2]. For an ideal $\mathfrak{N} \subset \mathcal{O}_K$

prime to disc(E), define

$$\psi(\mathfrak{N}) = \begin{cases} \left(\frac{6b\gamma_3}{\mathfrak{N}}\right)_{2,H} \epsilon_\tau(\pi)\pi & \text{if } D \text{ is odd} \\ \left(\frac{-6bi\gamma_3}{\mathfrak{N}}\right)_{2,H} \epsilon_\tau(\pi)\pi & \text{if } D \equiv 4, 8 \mod 16 \\ \left(\frac{6^2b^2(j-1728)}{\mathfrak{N}}\right)_{4,H} \epsilon_\tau(\pi)\pi & \text{if } D \equiv 0, 12 \mod 16 \end{cases}$$

Note that by construction we have

Lemma 2.4. *If $\mathfrak{N}$ is prime, then $\psi(\mathfrak{N})$ from Definition 2.3 and $\psi(\mathfrak{N})$ from Lemma 2.2 agree.*

Proof. This is Proposition 5.3 of [12]. □

2.3 The $\mathcal{O}_K$-module generated by P

Let $P \in E((\mathcal{O}_H/\mathfrak{N})[x]/(f_k))$. We now specify some of the details of the structure of the $\mathcal{O}_K$-module (P) generated by P. Let $\mathrm{ord}_{\mathfrak{N}}(P)$ denote the unique ideal such that $[\lambda]P \equiv O_E \mod \mathfrak{N}$ if and only if $\lambda \in \mathrm{ord}_{\mathfrak{N}}(P)$. In other words, $\mathrm{ord}_{\mathfrak{N}}(P)$ is the annihilator of (P). We must check this is well defined, and that we can say something about it computationally.

Lemma 2.5. *If $\mathfrak{N}$ is prime, $\mathrm{ord}_{\mathfrak{N}}(P)$ exists. Moreover, for some unit $u \in \mathcal{O}_K^\times$,*

$$\mathrm{ord}_{\mathfrak{N}}(P) \supset (uN_{H/K}(\mathfrak{N})^k - 1) = (\psi(\mathfrak{N})^k - 1).$$

To do this we need the help of two lemmata.

Lemma 2.6. *For all $P \in E((\mathcal{O}_H/\mathfrak{N})[x]/(f_k))$, $(\psi(\mathfrak{N})^k - 1)P = O_E$ if $\mathfrak{N}$ is prime.*

Proof. By definition, $\psi(\mathfrak{N}))[x_0 : y_0 : z_0] \equiv [x_0^n : y_0^n : z_0^n] \mod \mathfrak{N}$, where $n = \mathrm{char}\, \mathcal{O}_H/\mathfrak{N}$. We can write each projective coordinate as some polynomial $\sum_{i=0}^{k-1} a_i x^i$ in $(\mathcal{O}_H/\mathfrak{N})[x]/(f_k)$, with $a_i \in \mathcal{O}_H/\mathfrak{N}$. By the definition of f_k and a Galois extension, $(\sum_{i=0}^{k-1} a_i x^i)^n = \sum_{i=0}^{k-1} a_i \zeta_k^i x^i$ for some k-th root of unity $\zeta_k \in \mathcal{O}_H$. Then lemma follows when raising to the n-th power k times, since $[\psi(\mathfrak{N})^k]P \equiv P \mod \mathfrak{N}$. □

Now we introduce 2.7, using a similar methodology to [8] theorem 3.5 (a).

Lemma 2.7. *If $P \not\equiv O_E \mod \mathfrak{N}$ and $[\mathfrak{a}]P \equiv O_E \mod \mathfrak{N}$ for some ideal $\mathfrak{a}$ (if $[\lambda]P \equiv O_E \mod \mathfrak{N}$ for each $\lambda \in \mathfrak{a}$), and if there is an element $\lambda \in \frac{\mathfrak{a}}{\mathfrak{h}}$ such that $[\lambda]P \not\equiv O_E \mod \mathfrak{N}$, for each prime $\mathfrak{h}|\mathfrak{a}$, then*

$$[\lambda]P \equiv O_E \mod \mathfrak{N} \Leftrightarrow \lambda \in \mathfrak{a}.$$

Proof. Assume that $[\lambda]P \equiv O_E \mod \mathfrak{N}$. Then further assuming $\lambda \notin \mathfrak{a}$, we have that $[\gcd(\mathfrak{a}, \lambda End(E))]P \equiv O_E \mod \mathfrak{N}$. If $\gcd(\mathfrak{a}, \lambda End(E)) = (1)$ then we have a contradiction. So assume that $\gcd(\mathfrak{a}, \lambda End(E))$ is a proper ideal of $End(E)$. But then since $\gcd(\mathfrak{a}, \lambda End(E))|\mathfrak{a}$ and since $\lambda \notin \mathfrak{a}$ by assumption, we have that $\gcd(\mathfrak{a}, \lambda End(E)) \supsetneq \mathfrak{a}$, a contradiction because then for some prime $\mathfrak{h}|\mathfrak{a}$, $\gcd(\mathfrak{a}, \lambda End(E)) \supset \frac{\mathfrak{a}}{\mathfrak{h}}$. □

Proof of Lemma 2.5. If $\mathfrak{N}$ is prime then $[\lambda]P \equiv O_E \mod \mathfrak{N}$ for every $\lambda \in (\psi(\mathfrak{N}))^k - 1)$, by Lemma 2.6. If $[1]P = O_E \mod \mathfrak{N}$, then $(1) = \text{ord}_{\mathfrak{N}}(P)$, and the condition that $[\lambda]P \not\equiv O_E \mod \mathfrak{N}$ for $\lambda \notin (1)$, as well as uniqueness, is trivial. Otherwise we have that $[1]P \not\equiv O_E \mod \mathfrak{N}$. Then consider each prime $\mathfrak{h}|(\psi(\mathfrak{N})^k - 1)$, and the corresponding ideal $\mathfrak{h}^{-1}(\psi(\mathfrak{N})^k - 1) = \frac{(\psi(\mathfrak{N})^k-1)}{\mathfrak{h}}$. If for each $\mathfrak{h}$ we have that $[\lambda]P \not\equiv O_E \mod \mathfrak{N}$ for some $\lambda \in \mathfrak{h}^{-1}(\psi(\mathfrak{N})^k - 1)$, then we have $\text{ord}_{\mathfrak{N}}(P) = (\psi(\mathfrak{N})^k - 1)$ by Lemma 2.7. Alternatively, let i index through the distinct $\mathfrak{h}_i|(\psi(\mathfrak{N})^k - 1)$ such that $[\mathfrak{h}_i^{-1}\psi(\mathfrak{N})^k - 1)]P \equiv O_E \mod \mathfrak{N}$. Then $\text{ord}_{\mathfrak{N}}(P) = \frac{(\psi(\mathfrak{N})^k-1)}{\prod_i \mathfrak{h}_i}$ by construction and Lemma 2.7. This divides $(\psi(\mathfrak{N})^k - 1)$ and is unique again by Lemma 2.7.

□

2.4 Main Theoretical Results

To begin this section we should remark the following.

Remark 2.8. For $\mathfrak{p} \subset \mathcal{O}_H$, we have that $N_{H/\mathbb{Q}}(\mathfrak{p}) = p^j$ is a prime power. Thus if we first check that the integers N we test are not perfect powers, we can test the primality of $N = N_{H/\mathbb{Q}}(\mathfrak{N})$ by testing the primality of $\mathfrak{N}$.

Remark 2.9. The trial division steps in this section will be proven in the proceeding one. Additionally, an algorithm to complete the trial division will be given.

We now state our analogue of Lenstra's theorem for CM elliptic curves. First we state a straightforward lemma.

Lemma 2.10. *If $\mathfrak{p}$ is prime and we choose an f_k as defined in the definitions section, then*

$$[\psi(\mathfrak{p})]P = [\sigma_{G_p}x_0 : \sigma_{G_p}y_0 : \sigma_{G_p}z_0]$$

Proof. By definition, both $\psi(\mathfrak{p})$ and σ_{G_p} yield the coordinate-wise Frobenius. □

Theorem 2.11. *Let notation be as above and fix some $\mathfrak{N} \nmid (2)$. Assume that $N > 1 \neq n^r$ for some integer n and $r > 1$. Let $(\psi(\mathfrak{N})^k - 1) = \Gamma\Lambda$, with $\Lambda = (\lambda)$ principal, the primary factorization $\prod \mathfrak{q}^{e_q}$ of Λ known, and $N_{K/\mathbb{Q}}(\Lambda) > N^{1/2}$. If one can choose an f_k, and if $\exists P = [x_0 : y_0 : z_0] \in E((\mathcal{O}_F/\mathfrak{N})[x]/(f_k))$ such* *that*

(1) $[\lambda]P = O_E$,

(2) $[\lambda_{\mathfrak{q}}]P$ *is strongly nonzero modulo* $\mathfrak{N}$ *for each distinct prime* $\mathfrak{q}|\Lambda$, *where* $\lambda_{\mathfrak{q}}$ *is some element of* $\Lambda/\mathfrak{q}$,

(3) $[\psi(\mathfrak{N})]P = [\sigma_{G,j}x_0 : \sigma_{G,j}y_0 : \sigma_{G,j}z_0]$, *for some* j,

then $\psi(\mathfrak{p}) = \psi(\mathfrak{N})^m$ *in* $\mathcal{O}_K/(\Lambda)$ *for* $m = 1, ..., k$, *up to units. If further none of the* $O(4(-d)+4d^2)$ *residues* β *of* $\psi(\mathfrak{N})^m$, $m = 1, ..., k$ *with* $N_{K/\mathbb{Q}}(\beta) \leq N_{K/\mathbb{Q}}(\Lambda)$ *have that* $N_{K/\mathbb{Q}}(\beta)$ *properly divides* N, *then* N *is prime.*

Proof. Assume that conditions (1) and (2) hold for some prime $\mathfrak{q}|\Lambda$. Condition (1) yields that $\mathrm{ord}_{\mathfrak{p}}(P) \supset \mathfrak{q}^{v_{\mathfrak{q}}(\Lambda)}$ by definition of order, for each prime ideal $\mathfrak{p}|\mathfrak{N}$. Condition (2) yields that there is an element λ_{II} of $\Lambda/\mathfrak{q}$, and thus of $\mathfrak{q}^{v_{\mathfrak{q}}(\Lambda)-1}$ such that $[\lambda]P \not\equiv O_E \mod \mathfrak{p}$. Thus $\mathrm{ord}_{\mathfrak{p}}(P) \not\supset \mathfrak{q}^{v_{\mathfrak{q}}(\Lambda)-1}$ by definition of order. So we have that $\mathrm{ord}_{\mathfrak{p}}(P) \subset \mathfrak{q}^{v_{\mathfrak{q}}(\Lambda)}$ by primality. Note this holds for each $\mathfrak{q}|\Lambda$.

By condition (3), $[\psi(\mathfrak{N})]P = [\sigma_{G,j}x_0 : \sigma_{G,j}y_0 : \sigma_{G,j}z_0]$. By construction,

$$\sigma_{Gnj}^m z_0 \not\equiv z_0 \mod \mathfrak{p}, 1 \leq j < k$$

and further $\sigma_{G,j}^k z_0 \equiv z_0 \mod \mathfrak{p}$ (and similarly for x_0, y_0). By construction, $\sigma_{G,j}$ reduces modulo $\mathfrak{p}$ to an element of G_p, the Galois group G_p of the cyclic Galois extension $(\mathcal{O}_H/\mathfrak{p})[x]/(f_k)$. By the above analysis, and because G_p is cyclic (of order k), $\sigma_{G,j}$ generates G_p. But by Lemma 2.10, we have that $[\psi(\mathfrak{p})]P = [\sigma_{G_p}x_0 : \sigma_{G_p}y_0 : \sigma_{G_p}z_0]$, where $\sigma_{G_p} \in G_p$ is the Frobenius. By generation, $\sigma_{G_p} = \sigma_{G,j}^m$ for some $1 \leq j \leq k$. Thus

$$\begin{aligned}[\psi(\mathfrak{N})^m]P &\equiv [\sigma_{G,j}^m x_0 : \sigma_{G,j}^m y_0 : \sigma_{G,j}^m z_0] \\ &\equiv [\sigma_{G_p}x_0 : \sigma_{G_p}y_0 : \sigma_{G_p}z_0] \equiv [\psi(\mathfrak{p})]P \mod \mathfrak{p}\end{aligned}$$

Note that $[\psi(\mathfrak{N})]$ is guaranteed to commute with σ_G since we have reduced modulo a prime $\mathfrak{p}$. In particular we know that $[\psi(\mathfrak{N}^j) - \psi(\mathfrak{p})]P \equiv O_E \mod \mathfrak{p}$. By the results of the first paragraph and Lemma 2.5, $\psi(\mathfrak{N})^j - \psi(\mathfrak{p}) \in \text{II}^{e_q}$. Since this is true for each prime $\mathfrak{q}|\Lambda$, $\psi(\mathfrak{N})^j - \psi(\mathfrak{p}) \equiv 0 \mod \Lambda$.

Assume now that none of the residues β of $\psi(\mathfrak{N})^m$, $m = 1, ..., k$ modulo Λ with $N_{K/\mathbb{Q}}(\beta) \leq N^{1/2}$ have $N_{K/\mathbb{Q}}(\beta)|N$. Then for every distinct prime divisor $\mathfrak{p}|\mathfrak{N}$, $N_{K/\mathbb{Q}}(\psi(\mathfrak{N})) > N^{1/2}$ and $N_{K/\mathbb{Q}}(\psi(\mathfrak{N}))|N$. Clearly there can thus be only one distinct prime divisor $\mathfrak{p}$ of $\mathfrak{N}$. If $\mathfrak{p}^r = \mathfrak{N}$ for $r > 1$, then by norm multiplicativity, $N = p^r$, which is a contradiction since we assumed N was not a prime power. Thus $\mathfrak{N}$ is prime. Since we assumed N is not a prime power, N is also prime by Remark 2.8.

By Theorem 2.18, there are $O(4(-d) + 4d^2)$ residues to check for each given m.

□

In practice, an issue that arises with the initial test is that one must compute the action of the (non-integer) complex multiplication isogenies in precomputation. There is no repository of such isogenies known to the author online.

Additionally, the test, although a sufficient condition for primality, is not a necessary one, and one run runs in $\widetilde{O}(k^2 \log^3 N)$ (similar to Lenstra's criterion). We will now introduce the framework for a Las Vegas test for primality that runs in average time $\widetilde{O}(\log^2 N)$ on certain classes of integers, and certifies primality in one run through with nearly 100% probability for large inputs.

We begin with some lemmata. We say a solution to $x^k = 1$ is *k-primitive* if $x^m \neq 1$ for $0 < m < k$.

Lemma 2.12. *Let $\mathfrak{p}$ be a prime ideal which is not inert and $\mathfrak{p} \nmid 2$. Then $\mathcal{O}_K/\mathfrak{p}^n$ has is generated by one element when considered as a multiplicative group. In particular, if $x^k = 1$ in $\mathcal{O}_K/\mathfrak{p}^n$ has a k-primitive solution, then it has precisely k solutions.*

Lemma 2.13. *Let $N = \psi\overline{\psi}$ split in $\mathcal{O}_K$. Let n be a positive integer such that $(n)|\psi - 1$, then $N \equiv 1 \mod n$.*

Proof. If $(n)|\psi - 1$, then $(n = \overline{n})|(\overline{\psi - 1} = \overline{\psi} - 1)$. But then $N = \psi\overline{\psi} \equiv 1 \cdot 1 = 1$ mod n, as desired. □

Thus we do not lose much by taking $\mathfrak{q}$ to be non-inert. If it were inert in the following theorem, the classical finite fields test could be used. Further, it does not hurt to assume $(q^{e_q}) \nmid (\psi(\mathfrak{N})^k - 1)$, as otherwise $q^{e_q}|N^k - 1$ by Lemma 2.13 and the classical Lenstra primality test may be used.

Theorem 2.14. *Let notation be as above and fix some $\mathfrak{N} \nmid (2)$. Assume $N > 1$. Let $(\psi(\mathfrak{N})^k - 1) = \Gamma\mathfrak{q}^{e_q}$ with $\mathfrak{q} \nmid (2)$ a non-inert principal prime and $q^{e_q} := N_{K/\mathbb{Q}}(\mathfrak{q}^{e_q}) > N^{1/2}$. Further assume $((\psi(\mathfrak{N}))^m - 1) \notin \mathfrak{q}^{e_q}$ for $0 < m < k$, and that $(q^{e_q}) \nmid ((\psi(\mathfrak{N}))^k - 1)$. If there is an f_k with $P \in E((\mathcal{O}_H/\mathfrak{N})[x]/(f_k))$ such that*

(1) $[q^{e_q}]P = O_E$,
(2) $[q^{e_q-1}]P$ is strongly nonzero modulo $\mathfrak{N}$,

then $\psi(\mathfrak{p}) = \psi(\mathfrak{N})^m$ in $\mathcal{O}_K/\mathfrak{q}^{e_q}$ for some prime $\mathfrak{p}|\mathfrak{N}$ up to units. If further none of the $O(4(-d) + 4d^2)$ residues β of $\psi(\mathfrak{N})^m$, $m = 1, ..., k$ with $N_{K/\mathbb{Q}}(\beta) \leq N_{K/\mathbb{Q}}(\Lambda)$ have that $N_{K/\mathbb{Q}}(\beta)$ properly divides N, then N is prime.

Proof. Condition (1) gives $\text{ord}_{\mathfrak{p}}(P) \supset (q^{e_q})$ by definition, for every prime $\mathfrak{p}|\mathfrak{N}$. Condition (2) yields that there is an element λ of (q^{e_q-1}) such that $[\lambda]P \not\equiv O_E \mod \mathfrak{p}$ for each $\mathfrak{p}$ (the element λ is q^{e_q-1}). This implies that $\text{ord}_{\mathfrak{p}}(P) \not\supset (q^{e_q-1})$ and thus that $\mathfrak{q}^{e_q}|\,\text{ord}_{\mathfrak{p}}(P)$ or $\overline{\mathfrak{q}}^{e_q}|\,\text{ord}_{\mathfrak{p}}(P)$, for each $\mathfrak{p}|\mathfrak{N}$. Assume for contradiction that $\overline{\mathfrak{q}}^{e_q}|\,\text{ord}_{\mathfrak{p}}(P)|(\psi(\mathfrak{p})^k - 1)$ for each $\mathfrak{p}$. By Theorem 5.3 of [12], $\pi_{\mathfrak{p}}^k = u_p\psi(\mathfrak{p})^k$ for some unit $u_p \in \mathcal{O}_K^\times$. This implies that $\mathfrak{q}^{e_q}|(u_p\pi_{\mathfrak{p}}^k - 1)$ and thus that $\mathfrak{q}^{e_q}|(u_p^{v_p}\pi_{\mathfrak{p}}^{v_p k} - 1)$ where v_p is the highest power of $\mathfrak{p}$ dividing $\mathfrak{N}$ by norm multiplicativity. Again by multiplicativity, we see that

$$\mathfrak{q}^{e_q}|(u_p^{v_p}\pi_{\mathfrak{p}}^{v_p k} - 1) \Rightarrow \mathfrak{q}^{e_q}|(u\pi^k - 1)$$

for some unit u. By construction, $\psi(\mathfrak{N})) = u'\pi$ for some unit u', and thus

$$\begin{aligned}\psi(\mathfrak{p})^k - 1 &= u'^k\pi^k - 1\\ &= u\pi^k - u''\end{aligned}$$

for some unit u''. Note $u'' = \pm 1$. If $u'' = 1$ we have a contradiction, since $\overline{\mathfrak{q}}^{e_q}|\psi(\mathfrak{N})^k - 1$, and thus that $q^{e_q}|\psi(\mathfrak{N})^k - 1$, a contradiction by assumption. But $u'' = 1$ by construction of $\psi(\mathfrak{N})$. Fix this $\mathfrak{p}$.

We have by definition of f_k that $[\psi(\mathfrak{p})^k]P = P \mod \mathfrak{p}$ and thus that $\psi(\mathfrak{p})^k = 1$ in $\mathcal{O}_K/\mathfrak{q}^{e_q}$ by definition of order as the annihilator (Lemma 2.5). Since we have by choice that $\psi(\mathfrak{N})^k = 1$ and $\psi(\mathfrak{N})^m \neq 1$ in $\mathcal{O}_K/\mathfrak{q}^{e_q}$ for $0 < m < k$, and since by Lemma 2.12 there are precisely k elements e in $\mathcal{O}_K/\mathfrak{q}^{e_q}$ with $e^k = 1$, we have that said k elements are precisely $\psi(\mathfrak{N})^m$, $0 \leq m < k$. In particular, $\psi(\mathfrak{p}) = \psi(\mathfrak{N})^m$ in $\mathcal{O}_K/\mathfrak{q}^{e_q}$ for some $0 \leq m < k$.

The result then follows exactly as in Theorem 2.11.

□

To specify a primality test based on this theorem, we introduce some lemmata.

Lemma 2.15. *Let n be a positive integer not divisible by some non-inert $p =$ $\mathrm{char}(\mathbb{F}_q)$; then we have*

$$E[n] \subset E(\mathbb{F}_q) \Leftrightarrow (n)|\psi(\mathfrak{p}) - 1 \textit{ in } \mathcal{O}_K.$$

Proof. The backwards direction is straightforward. If $(n)|\psi(\mathfrak{p}) - 1$, then for $P \in E(\mathbb{F}_q)$ we have $[\psi(\mathfrak{p}) - 1]P = [n\gamma]P$ for some $\gamma \in \mathcal{O}_K$. But then if $P \in E[n]$, $[\psi(\mathfrak{p}) - 1]P = O_E \Rightarrow [\psi(\mathfrak{p})]P = [\psi(\mathfrak{p})][x : y : z] = [x^p : y^p : z^p] = [x : y : z] = P$.

The forward direction follows from [11].

□

We know that $ker([\mathfrak{q}^x]) = q^x$. Assume $\mathfrak{q}^x|\psi(\mathfrak{p})^k - 1$. In particular we thus have that $E[\mathfrak{q}^x] \subset E((\mathcal{O}_H/\mathfrak{p})[x]/(f_k))$ as rings. By [16], we have that, as groups,

$$E((O_H/\mathfrak{p})[x]/(f_k)) \simeq_\phi \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

where $n|m$ and the groups are additive. Denote $\#E_{p,k} = \#E((O_H/\mathfrak{p})[x]/(f_k)$. Assume $q^x|\#E_{p,k}$. By primality we have that $q^x|nm$ implies $q^{x-y}|n$, $q^y|m$. Since $n|m$, we must have that $y \geq x - y$, so we can take $y \geq x/2$. Thus we have

$$\left[\frac{\#E_{p,k}}{q^x}\right] P = O_E \Leftrightarrow (P \mapsto_\phi (a,b) :\ n|a \cdot \frac{\#E_{p,k}}{q^x} \text{ and } m|b \cdot \frac{\#E_{p,k}}{q^x})$$

Note that since $n, m|\#E_{p,k}$ $(nm = \#E_{p,k})$,

$$(P \mapsto_\phi (a,b) :\ n|a \cdot \frac{\#E_{p,k}}{q^x} \text{ and } m|b \cdot \frac{\#E_{p,k}}{q^x}) \Leftrightarrow (P \mapsto_\phi (a,b) :\ q^{x-y}|a \text{ and } q^y|b)$$

Wlog, $0 \leq a \leq n, 0 \leq b \leq m$. There are $\lfloor m/q^y \rfloor + 1$ such b that are multiples of q^y. This implies that randomly choosing $(a, b) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, the probability that $q^y | b$, $q^{x-y} | a$ (which is less than or equal to the probability that $q^y | b$) is at most

$$\begin{aligned} \frac{n(\lfloor m/q^y \rfloor + 1)}{nm} &\leq \frac{nm/q^y + n}{nm} \\ &= \frac{1}{q^y} + \frac{1}{m} \\ &\leq \frac{2}{q^{x/2}}. \end{aligned}$$

We can now show the following theorem.

Theorem 2.16. *Let $\mathfrak{N}$ be prime and satisfy the assumptions of Theorem 4, and further suppose $\psi(\mathfrak{N})^k - 1 = \Gamma\Pi^{e'}$ with $q^{e'} > N^{1/2+\alpha}$. Then for a randomly chosen Q, conditions (1), (2) are satisfied for*

$$P = \left[\frac{\#E_{p,k}}{q^{e'}}\right] Q$$

with probability at least $1 - \frac{1}{N^{\alpha/2}}$ for some e_q such that $N^{1/2} < q^{e_q} \leq q^{e'}$.

Proof. By the above discussion, if $\mathfrak{N}$ is prime then

$$\begin{aligned} [q^x]\, P &\equiv O_E \mod \mathfrak{N} \\ \Leftrightarrow \left[\frac{\#E_{p,k}}{q^{e'-x}}\right] Q &\equiv O_E \mod \mathfrak{N} \end{aligned}$$

occurs with probability at most $1/q^{e'-x}$. If we let $x = \lfloor N^{1/2}/q \rfloor$, then q^x is the largest power of q less than or equal to $N^{1/2}$ and $q^{e'-x} > N^\alpha$. Thus $[q^x]P \equiv O_E$ mod $\mathfrak{N}$ with probability at most $1/N^{\alpha/2}$ by the above discussion. If it is not the identity, then by the Lemma 2.5 and that $(q^{e'}) \subset \operatorname{ord}_{\mathfrak{N}}(P)$ and $(q^x) \not\subset \operatorname{ord}_{\mathfrak{N}}(P)$, $q^{e_q} = \operatorname{ord}_{\mathfrak{N}}(P)$ with $q^{e_q} > N^{1/2}$ by definiton of x, satsifying condition (1) for e_q. Condition (2) is satisfied for $e_q - 1$ since by choice of e_q, $[q^{e_q - 1}]P \not\equiv O_E$ mod $\mathfrak{N}$, and since $\mathfrak{N}$ is prime, this yields strongly-nonzero modulo $\mathfrak{N}$. □

If the test fails to certify primality or prove compositness in one run through with a non-negligible α, then the number is very likely composite, so utilize the Miller-Rabin compositness test, which has an average runtime of $\widetilde{O}(\log^2 N)$ [17]. This provides a quasi-quadratic Las Vegas algorithm for primality of a new class of integers with an average runtime of $\widetilde{O}(\log^2 N)$, and furthermore that certifies primes in $\widetilde{O}(\log^2 N)$ with probability $1 - 1/N^{\alpha/2}$, which is nearly 1 for large N, non-negligible α.

2.5 Residue Classes in Non-Euclidean Quadratic Rings

Let $K = \mathbb{Q}[\sqrt{d}]$ be a quadratic number field, with d squarefree, equipped with the standard norm $|\bullet|$. Let $\mathfrak{I} \subset \mathcal{O}_K$ be an ideal. For $\alpha \in \mathcal{O}_K$, let $\overline{\alpha}$ denote the image of α under the quotient map $\phi_{\mathfrak{I}} : \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{I}$. In this section we seek for $\overline{\beta} \in \mathcal{O}_K/\mathfrak{I}$ to find all lifts $\phi_{\mathfrak{I}}^{-1}(\overline{\beta})$ with norms below a certain bound.

For the purposes of this paper, we will assume that $\mathfrak{I} = (\iota)$ is principal. We will also restrict to the case of $d < 0$ as we will be working with imaginary quadratic number fields. It is well known that for $d < 0$, there are only finitely many norm-Euclidean $\mathcal{O}_K$:

Theorem 2.17. *The norm-Euclidean quadratic number fields with $d < 0$ are precisely given by*

$$d = -1, -2, -3, -7, -11.$$

For these quadratic number fields alone we can in general guarantee and determine a lift $\phi_{\mathfrak{I}}^{-1}(\overline{\beta})$ such that $|\phi_{\mathfrak{I}}^{-1}(\overline{\beta})| < |\iota|$. For other d, such a lift may not exist. We consider in this section the following theorem.

Theorem 2.18. *Let $K = \mathbb{Q}[\sqrt{d}]$ for $d < 0$ squarefree. Again let $\overline{\beta} \in \mathcal{O}_K/\mathfrak{I}$ with $\mathfrak{I} = (\iota)$ principal. Then there exist $O(4(-d) + 4d^2)$ lifts $\phi_{\mathfrak{I}}^{-1}(\overline{\beta})$ such that $|\phi_{\mathfrak{I}}^{-1}(\overline{\beta})| \leq |\iota|$. Furthermore they may be found or ruled out in deterministic $O(4(-d) + 4d^2)$ steps.*

Note that the lifts $\phi_{\mathfrak{I}}^{-1}(\overline{\beta})$ are given precisely by $\iota X + \beta$ for $X \in \mathcal{O}_K$ and a choice of lift, β, since $\mathfrak{I} = (\iota)$. In general, we have the following lemma.

Lemma 2.19. *Let $\iota, \beta, X \in \mathcal{O}_K$ be any elements. Assume $|X| \geq 4(-d) + 4d^2$ and $(-d + d^2)|\iota| \geq |\beta|$. Then $|\iota X + \beta| \geq |\iota|$.*

Proof. If for a positive constant k, $|X| \geq k(-d) + kd^2$, then by multiplicativity of field norms, $|\iota X| \geq (k(-d) + kd^2)|\iota|$. Then we can write $\iota X = a + b\sqrt{d}$ with $a^2 + b^2(-d) = |\iota X| \Rightarrow a^2 \geq |\iota X|/2$ or $b^2(-d) \geq |\iota X|/2$. Writing $\beta = c + e\sqrt{d}$, we have an analogous inequality. Thus we have that

$$\begin{aligned}
|\iota X + \beta| &\geq \max((|a| - |c|)^2, (|b| - |e|)^2 d) && \text{since } |x + y\sqrt{d}| \geq x^2, y^2 d \text{ for } d < 0,\\
&\geq \left(\sqrt{|\iota X|/2} - \sqrt{(-d + d^2)|\iota|/2}\right)^2 && \text{since } |\beta| \leq (-d + d^2)|\iota|,\\
&\geq \left(\sqrt{|\iota|(-kd + kd^2)/2} - \sqrt{(-d + d^2)|\iota|/2}\right)^2 && \text{by assumption,}\\
&= 1/2(-1 + d)d(-1 + \sqrt{k})^2|\iota|.
\end{aligned}$$

We want $1/2(-1 + d)d(-1 + \sqrt{k})^2 \geq 1$, and for all d it suffices to choose $k = 4$. □

To prove theorem 2.18, the general idea is, given a representative $\overline{\beta}$ of an equivalence class, find a new representative of the same equivalence class, β, with $(-d + d^2)|\iota| \geq |\beta|$, and then to apply theorem 2.18. Let $\iota = a + b\sqrt{d}$. One may naively attempt to consider the image of $\overline{\beta}$ under the surjection with kernel

$|\iota| \in \mathfrak{I}$, but this in worst case has $|\beta| = (|\iota|-1+\sqrt{d}(|\iota|-1))^2 \sim |\iota|^2$. Attempting to modify Lemma 2.19 to allow this larger bound yields that we must take that $|X|$ grows with $|\iota|$, which prohibits iterating through the lifts $\iota X + \beta$ for large $|iota|$.

Consider instead a coordinate plane with horizontal axis the real line and vertical axis given by real multiples of $\sqrt{d}$. Thus a point (x, y) represents $x + y\sqrt{d}$. Form a new grid with sides $1(\iota) = a + b\sqrt{d}, -1(\iota) = -a - b\sqrt{d}, \sqrt{d}\iota = bd + a\sqrt{d}, -\sqrt{d}\iota = -bd - a\sqrt{d}$ by applying the change of coordinates matrix

$$\begin{bmatrix} a & -bd \\ b & -a \end{bmatrix}$$

to the plane. Each grid square now represents all distinct classes of elements of $\mathcal{O}_K$ modulo (ι). In particular, in this new coordinate system, moving one step in any direction corresponds to adding a multiple of ι and thus adding 0 mod (ι).

To transform $\overline{\beta} = c + e\sqrt{d}$ into these coordinates, solve

$$\begin{bmatrix} c \\ e \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix} A + \begin{bmatrix} b(-d) \\ -a \end{bmatrix} B$$

for (A, B). Then consider $(A', B') = (A - \lfloor A \rfloor, B - \lfloor B \rfloor)$. Then take

$$\beta = A' \begin{bmatrix} a \\ b \end{bmatrix} + B' \begin{bmatrix} b(-d) \\ -a \end{bmatrix}$$

as a representative of the same equivalence class as $\overline{\beta}$ (since we have subtracted elements of ι), that lies within the four grid boxes nearest the origin (those with coordinates $(\pm 1, \pm 1)$). Importantly, each both the real and imaginary parts of β are bounded above in magnitude by the magnitude of the real and imaginary parts of the four coordinate boxes (given in the new coordinates by $(\pm 1, \pm 1)$) nearest the origin:

$$\begin{aligned} |\beta| \le |\max(|bd|, |a|) + \sqrt{d}\max(|a|, |b|)| &\le \max(a^2(1 + (-d)), b^2d^2(1 + (-d))) \\ &\le d^2b^2(1-d) - da^2(1-d) = |\iota|| - d + d^2| \end{aligned}$$

In particular this element β satisfies the norm size constraint of Lemma 2.19. This suffices to prove 2.18 as seen in the next section.

3 Implementation and Runtime

We now provide a Las Vegas algorithm for primality of a new class of integers that runs in average quasi-quadratic time and further certifies the primality of a prime input in quasi-quadratic time for almost all choices of input paramters.

From the discussion in the previous section, we get the following algorithm which proves Theorem 2.18:

Algorithm 3.1.

```
1. $K = \mathbb{Q}[\sqrt{d}], \overline{\beta} \in \mathcal{O}_K/(\iota), \iota = a + b\sqrt{d}, \overline{\beta} = c + e\sqrt{d}$
2. Compute $(A, B) =$ the solution of $\begin{bmatrix} c \\ e \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix} A + \begin{bmatrix} b(-d) \\ -a \end{bmatrix} B$
3. Compute $(A', B') = (A - \lfloor A \rfloor, B - \lfloor B \rfloor)$ to sufficient precision
4. Compute $\beta = A' \begin{bmatrix} a \\ b \end{bmatrix} + B' \begin{bmatrix} b(-d) \\ -a \end{bmatrix}$
5. Initialize return values $\{\}$
6. For all integers $0 \leq N, M < \sqrt{4(-d) + 4d^2}$,
   if $|(N + \sqrt{d}M)\iota + \beta| \leq |\iota|$, append $\{(N, M)\}$ to the result values
7. Return the result values
```

Proposition 3.2. Algorithm 3.1 runs in $O(4(-d) + 4d^2)$ steps.

Proof. Inspection. □

We now seek to implement the Las Vegas test based on Theorem 2.14 and the subsequent discussion. We will utilize notation as in Theorem 2.14. Before beginning the following algorithm, compute $\psi(\mathfrak{N})^k$ utilizing the results of the section Hecke Character Properties; the runtime of this step is dominated by that of the following algorithm.

Algorithm 3.3. Let notation be as above and fix some $\mathfrak{N} \nmid (2)$. Assume $N > 1$. Let $(\psi(\mathfrak{N})^k - 1) = \Gamma \mathfrak{q}^{e'}$ with $\mathfrak{q} \nmid (2)$ a non-inert principal prime and $q^{e'} := N_{K/\mathbb{Q}}(\mathfrak{q}^{e'}) > N^{1/2+\alpha}$. Further assume $((\psi(\mathfrak{N}))^m - 1) \notin \mathfrak{q}^y$ for $0 < m < k$ and $\mathfrak{q}^y > N^{1/2}$, and that $(q^y) \nmid ((\psi(\mathfrak{N}))^k - 1)$. Choose an f_k.

```
1. Choose some $Q \in E((\mathcal{O}_H/\mathfrak{N})[x]/(f_k))$
2. Compute $P = \left[\frac{\#E((\mathcal{O}_H/\mathfrak{N})[x]/(f_k))}{\mathfrak{q}^{e_q}}\right] Q \mod \mathfrak{N}$
If $q$ is sufficiently small :
a. Compute $[q^x]P \mod \mathfrak{N}$, storing the value until $[q^{x+2}]P \mod \mathfrak{N}$ is computed,
for $x = 0, 1, ..., e'$ until $[q^x]P \equiv O_E \mod \mathfrak{N}$.
If this does not hold for any such $x$, then return COMPOSITE
b. Check that $[q^{x-1}]P$ is strongly nonzero modulo $\mathfrak{N}$
If this does not hold, then return COMPOSITE
c. Check if $q^x > N^{1/2}$. If so, return POSSIBLY PRIME
If not, return PROBABLY COMPOSITE
```

Remark 3.4. If the algorithm terminates on step *a*., then $\mathfrak{N}$ is clearly composite, as a non-trivial ideal divisor was found. If the algorithm returns POSSIBLY

PRIME on step c., then the trial division algorithm must be run. If the algorithm returns PROBABLY COMPOSITE on step c., then by Theorem 2.16, $\mathfrak{N}$ is probably composite.

Remark 3.5. We can compute computations modulo $\mathfrak{N}$ by simply partially reducing modulo $N = N_{H/\mathbb{Q}}(\mathfrak{N})$. Then when checking whether some point $P = [x_0 : y_0 : z_0] \equiv O_E \mod \mathfrak{N}$, one can for example check that $\gcd(a_i\mathcal{O}_H, \mathfrak{N}) = \mathfrak{N}$ in $\mathcal{O}_H$ for each a_i in $z_0 = \sum_{i=0}^{k-1} a_i x^i$.

Remark 3.6. A similar algorithm can be developed for the more general case, but complex isogenies must be precomputed, and one must test multiple strongly nonzero conditions, increasing the complexity.

Proposition 3.7. Algorithm 3.3 is quasi quadratic in $c = O(\log N)$ for a fixed k.

Proof. The complexity of computing the integer isogenies in the elliptic curve group is the cost of binary exponentiation in $(\mathcal{O}_H/\mathfrak{N})[x]/(f_k)$ by the normal formula for integer isogenies of elliptic curves, which is $O(mM)$, where m is the number of bits in the largest exponent, M is the cost of mutliplication. The number of bits in the exponent is at most the log of the size of the group of points, which by the Hasse-Weil bound yields $O(kc) = O(c)$ by k being fixed. The cost of multiplication given remark 3.5 is $O(k^2(2)^2 \log N \log\log N)$ with $K = \sqrt{d}$ by using the Schonhage-Strassen algorithm on the real and imaginary parts of elements of $\mathcal{O}_H$ [19]. notice that the other steps are dominated by this exponentiation. Thus the complexity is $O(c^2 \log c)$ for fixed k. □

As alluded to above, if POSSIBLY PRIME is returned, run Algorithm 3.1 for K, $\psi(\mathfrak{N})^m$, $0 \leq m \leq k-1$, and $(\iota) = \text{II}$. Check if the norms of any of the results in the result values divide N. If not, return PRIME. If one does, return COMPOSITE.

Proposition 3.8. If PRIME is returned, then N is prime. If COMPOSITE is returned, then N is composite.

Proof. All we must check is the prime case, which follows from Theorem 2.14 and the subsequent discussion. □

The remaining case is when PROBABLY COMPOSITE is returned. In this case by Lemma 2.16, with probability at least $1 - 1/N^{\alpha/2}$, N is composite. Thus run it through the Miller-Rabin compositeness test, which proves a number is composite in average $O(\log^2 N)$ time [17]. If this does not terminate in $c' \log^2 N$ for some small c', utilize the AKS primality test which runs in $\widetilde{O}(\log^6 N)$ [10].

Theorem 3.9. *Fix K, k. Choose a random Q as above. Running Algorithm 3.3 for an N that satisfies its conditions, along with the subsequent discussion yields a Las Vegas algorithm for primality with average runtime $\widetilde{O}(\log^2 N)$ for large enough α. Further if N is prime, it is proven prime in $\widetilde{O}(\log^2 N)$ time for $1 - 1/N^{\alpha/2}$ of the input parameters Q.*

Proof. The runtime of Algorithm 3.1 is dominated by that of Algorithm 3.3 for fixed $K = \mathbb{Q}[\sqrt{d}]$. By the above analysis, if PRIME or COMPOSITE is returned before the AKS primality test is used, we have a runtime of $\widetilde{O}(\log^2 N)$. The AKS primality test has to be used for a prime input N with probability less than or equal to $1/N^{\alpha/2}$. Thus if N is prime the runtime is $O((1 - 1/N^{\alpha/2})\widetilde{O}(\log^2 N) + 1/N^{\alpha/2}\widetilde{O}(\log^6 N))$. If $\alpha \leq 1$ is large enough, this runtime is quasi-quadratic. It is known that the average runtime of the Miller Rabin compositeness test is $\widetilde{O}(\log^2 N)$ for composite N [17]. Thus if N is composite, the overall runtime is quasi-quadratic as well. □

4 Acknowledgements

I would like to thank Andrew Sutherland for his guidance on this paper and mentorship in general on elliptic curves, number theory, and algebraic geometry.

References

[1] S. Goldwasser and J. Kilian, Almost all primes can be quickly certified, Proc. 18th STOC (Berkeley,May 28-30, 1986),ACM, New York, 1986,pp. 316-329.

[2] Atkin, A. Oliver L., and François Morain. "Elliptic curves and primality proving." Mathematics of computation 61.203 (1993): 29-68.

[3] Pomerance, Carl. "Primality testing: variations on a theme of Lucas." Congr. Numer 201 (2010): 301-312.

[4] Lenstra, H. W. "Primality testing algorithms [after Adleman, Rumely and Williams]." Séminaire Bourbaki vol. 1980/81 Exposés 561–578. Springer, Berlin, Heidelberg, 1981. 243-257.

[5] Grau, José, Antonio Oller-Marcén, and Daniel Sadornil. "A primality test for $Kp^n + 1$ numbers." Mathematics of Computation 84.291 (2015): 505-512.

[6] Grau, J. M., A. M. Oller-Marcén, and D. Sadornil. "A primality test for $4Kp^n - 1$ numbers." Monatshefte für Mathematik 191.1 (2020): 93-101.

[7] Morain, François. "Implementing the asymptotically fast version of the elliptic curve primality proving algorithm." Mathematics of Computation 76.257 (2007): 493-505.

[8] Abatzoglou, Alexander, et al. "A framework for deterministic primality proving using elliptic curves with complex multiplication." Mathematics of Computation 85.299 (2016): 1461-1483.

[9] Abatzoglou, Alexander, et al. "Deterministic elliptic curve primality proving for a special sequence of numbers." The Open Book Series 1.1 (2013): 1-20.

[10] Agrawal, Manindra, Neeraj Kayal, and Nitin Saxena. ”PRIMES is in P.” Annals of mathematics (2004): 781-793.

[11] Rück, Hans-Georg. ”A note on elliptic curves over finite fields.” Mathematics of Computation 49.179 (1987): 301-304.

[12] Rubin, Karl, and Alice Silverberg. ”Point counting on reductions of CM elliptic curves.” Journal of Number Theory 129.12 (2009): 2903-2923.

[13] Crandall, Richard, and Carl Pomerance. Prime numbers. Telos, 2001.

[14] Mihailescu, Preda. ”Dual elliptic primes and applications to cyclotomy primality proving.” arXiv preprint arXiv:0709.4113 (2007).

[15] Lemmermeyer, Franz. Reciprocity laws: from Euler to Eisenstein. Springer Science & Business Media, 2013.

[16] Washington, Lawrence C. Elliptic curves: number theory and cryptography. Chapman and Hall/CRC, 2008.

[17] Conrad, Keith. ”The Miller–Rabin Test.” Encyclopedia of Cryptography and Security (2011).

[18] Onuki, Hiroshi. ”A primality proving using elliptic curves with complex multiplication by imaginary quadratic fields of class number three.” arXiv preprint arXiv:2211.15137 (2022).

[19] Schönhage, Arnold, and Volker Strassen. ”Schnelle multiplikation grosser zahlen.” Computing 7.3 (1971): 281-292.