When Elliptic-Curve Semiprimality Certificates Reveal Factors*

Giuseppe Vitto

LayerZero Labs

Abstract. Public certificates of semiprimality could support cryptographic modulus generation by proving that an integer has exactly two prime factors without revealing them. Their usefulness in this setting depends on whether the certificate preserves the difficulty of factoring. Motivated by the examples of Reble and Broadhurst, we formalize semiprimality certificates by adapting the Goldwasser–Kilian primality criterion. For certificates with a prime point order, our semiprimality theorem uses public data (N, S, E, P) comprising a composite nonsquare integer N, an elliptic curve E over $\mathbb{Z}/N\mathbb{Z}$, a certified prime $S > (N^{1/6} + 1)^2$, and a point $P \in E(\mathbb{Z}/N\mathbb{Z})$ of order S modulo every prime divisor of N. Hasse's bound forces each prime divisor above $N^{1/3}$, proving that N has exactly two prime factors. For such semiprimality certificates constructed using complex multiplication (CM), we show that a norm-lattice reconstruction factors N from (N, S, D) alone in expected polynomial time when the Frobenius at every prime divisor lies in a known imaginary quadratic field of fundamental discriminant D or has trace zero, and $\gcd(S, 2DN) = 1$. Applying this reconstruction and complementary public-point and quadratic-twist attacks, we factor Reble's 1084-digit and Broadhurst's 5061-digit moduli. These attacks also defeat proposed repairs based on hidden cofactors, withheld CM maps, or private isogeny descent within a known field under the stated hypotheses. We leave open whether one can efficiently produce a public Goldwasser–Kilian-based certificate for a fixed modulus, using its privately known factors, while preserving its factoring difficulty relative to the General Number Field Sieve.

Keywords: semiprimality certificates · integer factorization · complex multiplication

1 Introduction

In 2005, Reble and Broadhurst published elliptic-curve certificates for semiprimes of 1084 and 5061 digits [24,4]. Their certificates allow anyone to verify that the given integer has exactly two distinct prime factors, without listing those

* This manuscript develops and formalizes the preliminary ideas on semiprimality certificates in the author's 2021 preprint [29], and introduces new factoring attacks that revise its security assessment.

factors. This form of public verification is appealing for cryptographic modulus generation, where a verifier may need assurance about the arithmetic structure of a modulus while its factorization must remain secret.

For this purpose, however, the information disclosed by a certificate matters as much as the claim it proves. Even when the factors do not appear explicitly, the auxiliary curve and point may impose enough constraints to recover them. A certificate can therefore establish semiprimality correctly while making the modulus unsuitable for its intended cryptographic use. The construction question motivating this paper is: *Can one use the privately known factors of a fixed modulus to efficiently construct a public elliptic-curve semiprimality certificate while preserving the difficulty of factoring that modulus?*

We formalize the certificate criterion by adapting the primality criterion of Goldwasser and Kilian [14, Lemma 2]. Section 2 defines the public verification conditions and proves that they imply semiprimality, including variants that combine several certified prime orders. With correctness established, we turn to the information these conditions reveal about the unknown factors. The common order used to certify semiprimality is also the starting point for our factor-recovery attacks.

Attacks from Public Order Information. Our main result concerns certificates constructed using complex multiplication (CM), a method for building elliptic curves using the arithmetic of imaginary quadratic fields. For the class of prime-order certificates specified in Theorem 2, we show that the modulus N, the certified subgroup order S, and the discriminant D identifying the known field suffice to recover the factors in expected polynomial time. Thus the information needed for recovery can be much smaller than the certificate itself: the attack uses only these three integers, regardless of how the curve and point were constructed.

The key step is to extract arithmetic constraints on the unknown factors from the common subgroup order. We use these constraints to build a two-dimensional norm lattice whose relevant points can be enumerated efficiently, giving a direct reconstruction algorithm. Section 3 states the precise hypotheses and proves the result.

We complement this result with attacks that use the published point or additional information about the full curve orders. The public-point method also covers Gaussian certificates with composite point orders whose prime factorization is known. Together, these methods recover the factors of Reble's 1084-digit and Broadhurst's 5061-digit moduli [24,4]. Broadhurst's modulus also factors from N, S alone by norm reconstruction.

For the Boudabra–Nitaj RSA variant, we refute the claim in Section 6.4 and Section 6.5, Remark 1, of their paper [3] that difficulty in factoring the local curve-order product prevents factor recovery once that product is known. Under a twist-separation condition, it permits factoring the modulus directly (Section 7).

Attempted Repairs and the Construction Question. The small recovery input explains why withholding more of the construction does not necessarily repair

these certificates. Within the theorem's scope, private auxiliary parameters cannot protect the factors when the public subgroup order and known field already determine enough information to recover them. We show that this remains a problem for several proposed changes to the curve construction, including attempts to conceal the original curve while retaining the same known CM field. The later sections analyze these proposals and explain which features of the public certificate preserve the attack.

Constructions outside the theorem's hypotheses require separate analysis. We investigate alternatives that use different fields at the two prime factors and find that some still disclose enough information to distinguish and recover those factors. Experiments demonstrate this additional attack on the tested constructions with moduli of up to 4000 bits. The more general possibilities remain open.

For a future construction, the concrete security target is that its certificate offer no factoring attack cheaper than the General Number Field Sieve (GNFS) on the same N. Whether this target can be met remains open.

Related Work. The reconstruction connects certificate data to established algorithms for finding divisors subject to congruence constraints. Lenstra's residue-class divisor algorithm [20] and Hales's extension to norm-Euclidean imaginary quadratic rings [15] provide related reconstruction tools. For certificates using the Gaussian integers, our reduction allows recovery through Hales's algorithm. For arbitrary imaginary quadratic fields, it also allows polynomial recovery through Cohn–Heninger's number-field small-root theorem [8, Theorem 1.3 of the full version]; Appendix A details the latter reduction. Our contribution is to derive the required relations from semiprimality certificates and show that (N, S, D) suffices for recovery. Alongside these reductions to prior algorithms, we give a direct norm-lattice reconstruction and examine the consequences for certificate construction and use.

Our other attacks also build on earlier factoring methods. In particular, recovering factors by quadratic twisting when multiples of curve orders are available is classical [23,13]; Galbraith and McKee also give a reconstruction from a common order for a special class of curves [13, Section 5]. Other reductions obtain factors through point-counting or point-order oracles [17,21,11]; these results rely on oracle access, and in some cases additional divisibility assumptions, that differ from the public certificate data considered here. Earlier CM factoring methods use specially chosen curves and prescribed curve orders at the prime factors [6,25,1]. We use standard quadratic ideal arithmetic and CM theory as developed in [26,9,7].

Paper Organization. We begin with the certificate criterion in Section 2, then derive the norm-lattice reconstruction in Section 3. Sections 4 and 5 develop the quadratic-twist and public-point methods, including recovery from factored composite point orders. With these methods in place, we examine certificate construction in Section 6 and applications to elliptic-curve encryption in Section 7. Section 8 brings together the computational results, followed by the remaining construction limits and the comparison with GNFS in Section 9.

2 Semiprimality Certificates

We call $N = pq$ a *semiprime* when p and q are distinct primes. Squares are easy to recognize and factor, so we exclude them. Write $\mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z}$ and $\mathcal{O}$ for the identity of an elliptic curve. For a short Weierstrass model $E : y^2 = x^3 + Ax + B$, *good reduction* at a prime ℓ means that reducing the equation modulo ℓ gives a nonsingular curve, so it remains an elliptic curve over $\mathbb{F}_\ell$. We require $\gcd(N, 6\Delta_E) = 1$, where $\Delta_E = -16(4A^3 + 27B^2)$. This ensures good reduction at every prime divisor ℓ of N and excludes characteristics two and three. Its points over $\mathbb{F}_\ell$, including $\mathcal{O}$, form a finite abelian group $E(\mathbb{F}_\ell)$. We write $[k]P$ for scalar multiplication by an integer k, and $\#E(\mathbb{F}_\ell)$ for the group order. The order of a point is the least positive k for which $[k]P = \mathcal{O}$. Hasse's theorem states that

$$\big|\#E(\mathbb{F}_\ell) - (\ell + 1)\big| \le 2\sqrt{\ell};$$

see [27, Theorem V.1.1]. This bound connects a publicly certified point order to the size of every unknown prime factor. Throughout, logarithms are natural unless a base is specified.

Definition 1 (Strongly Nonzero Point). *A point $P \in E(\mathbb{Z}_N)$ is strongly nonzero if its reduction is not $\mathcal{O}$ at any prime divisor of N.*

Definition 2 (Elliptic-Curve Semiprimality Certificate). *For a composite, nonsquare integer N, a certificate consists of a curve $E/\mathbb{Z}_N$ with good reduction at every prime divisor of N, distinct primes $s_1, \dots, s_k$ with primality certificates, and strongly nonzero points $P_1, \dots, P_k$ such that*

$$[s_i]P_i = \mathcal{O} \quad (1 \le i \le k), \qquad M := \prod_{i=1}^{k} s_i > (N^{1/6} + 1)^2. \tag{1}$$

A verifier checks these conditions and verifies that N is composite and nonsquare.

Theorem 1 (Soundness). *Every composite, nonsquare integer so certified is semiprime.*

Proof. For every prime $\ell \mid N$, each reduced point has exact order s_i. The distinct primes s_i therefore all divide $\#E(\mathbb{F}_\ell)$, and their product M divides it. Hasse's bound gives

$$M \le \#E(\mathbb{F}_\ell) \le (\sqrt{\ell} + 1)^2, \qquad \ell \ge (\sqrt{M} - 1)^2 > N^{1/3}.$$

If N had at least three prime factors counted with multiplicity, their product would exceed N. Compositeness leaves exactly two; the nonsquare condition makes them distinct.

More generally, for any integer $m \ge 2$, the same argument shows that if $M > (N^{1/(2m)} + 1)^2$, then N has at most $m - 1$ prime factors counted with multiplicity.

Theorem 1 would fail if the certificate required only $P_i \neq \mathcal{O}$ over $\mathbb{Z}_N$, rather than strongly nonzero points. For example, over $N = 5705 = 5 \cdot 7 \cdot 163$, the curve $y^2 = x^3 + x$ has the projective point $P = (3185 : 2871 : 490)$. It reduces to the identity modulo 5 and 7, but to $(88, 100)$ of order 41 modulo 163. Thus $P \neq \mathcal{O}$ and $[41]P = \mathcal{O}$, with $41 > (N^{1/6} + 1)^2$, even though N has three prime factors. The scalar relation constrains the factor 163 but gives no order information at 5 or 7, where the point is already the identity. Requiring P to be strongly nonzero excludes this example; its projective denominator also exposes a factor through $\gcd(490, N) = 35$.

Composite Orders. An alternative certificate specifies an order $M = \prod_i s_i^{e_i}$ with certified prime factorization and a point P with $[M]P = \mathcal{O}$, and requires $[M/s_i]P$ to be strongly nonzero for every prime $s_i \mid M$. Then P has exact order M in every residue field, and the same soundness proof applies.

Our main theorem uses the common local order supplied by one prime S and one point P, so $M = S$. Recovery itself does not use P. The primality proof for S can itself be an elliptic-curve certificate, verified recursively [2, Section 10 of the preprint]. A probable-prime test leaves soundness conditional on the primality of S.

2.1 Complex Multiplication and Local Construction

An endomorphism is an algebraic map from a curve to itself that preserves the group law. Integer scalar multiplications are examples. A curve in characteristic ℓ is ordinary when it has a nonidentity point annihilated by ℓ over the algebraic closure, and supersingular otherwise. For an ordinary elliptic curve over $\mathbb{F}_\ell$, its geometric endomorphism ring is an order in an imaginary quadratic field K. An order is a subring of finite index in the ring of integers $\mathcal{O}_K$; it has the form $\mathcal{O}_f = \mathbb{Z} + f\mathcal{O}_K$ for a positive integer f, called its conductor. If D is the fundamental discriminant of K, the order discriminant is $\Delta = f^2 D$. The case $f = 1$ is the maximal order. We use CM for this quadratic endomorphism structure and for characteristic-zero curves with such endomorphisms.

The Frobenius endomorphism sends (x, y) to (x^ℓ, y^ℓ). In the ordinary case it corresponds to an algebraic integer $\pi_\ell \in \mathcal{O}_K$ satisfying

$$\pi_\ell^2 - t_\ell \pi_\ell + \ell = 0, \qquad \mathrm{Norm}(\pi_\ell) = \ell, \qquad \#E(\mathbb{F}_\ell) = \mathrm{Norm}(\pi_\ell - 1) = \ell + 1 - t_\ell.$$

Here t_ℓ is its trace and Norm is the quadratic field norm. These identities explain why a common curve-order divisor yields congruences for Frobenius; see [28, Section 2.11]. Supersingular curves have a different endomorphism algebra. Supersingularity implies $\ell \mid t_\ell$; Hasse's bound and $\ell > 3$ therefore force $t_\ell = 0$ and order $\ell + 1$. See [27, Theorem V.3.1 and Exercise V.5.10].

Combining Local Witnesses. When the factors p, q are known, a certificate can be assembled from curves and points constructed separately over $\mathbb{F}_p$ and $\mathbb{F}_q$. Suppose that the two curve orders share a certified prime divisor $S > (N^{1/6}+1)^2$.

On each curve, choose a nonidentity point satisfying $[S]P = \mathcal{O}$, that is, a nonzero point in its S-torsion subgroup. The Chinese remainder theorem (CRT) combines the curve coefficients and point coordinates into a curve and point over $\mathbb{Z}_N$. The resulting point has order S at both prime factors and is therefore strongly nonzero, as required by the certificate definition. The common divisor is essential here: if S divides only one curve order, every point satisfying $[S]P = \mathcal{O}$ reduces to the identity at the other factor.

To find the required points, write $n_p = \#E_p(\mathbb{F}_p)$ and $n_q = \#E_q(\mathbb{F}_q)$ for the two curve orders. For each $\ell \in \{p, q\}$, one can try multiplying a point on E_ℓ by the cofactor n_ℓ/S. The result satisfies $[S]P_\ell = \mathcal{O}$; if it is nonidentity, it has exact order S and can be used in the CRT construction. Multiplying a point over $\mathbb{Z}_N$ by $n_p n_q/S$ instead always gives the identity, because this scalar is a multiple of both curve orders. If S divides each order exactly once, the smaller scalar $n_p n_q/S^2$ can instead be used to seek a point over $\mathbb{Z}_N$, but its reductions must still be checked to be nonidentity at both factors.

For our controlled generation experiments, CM provides a way to arrange the common divisor S before searching for compatible primes p, q. Over the Gaussian integers $\mathbb{Z}[i]$, the norm is $\mathrm{Norm}(a + bi) = a^2 + b^2$. Choosing $\sigma, \alpha, \beta \in \mathbb{Z}[i]$ with

$$\mathrm{Norm}(\sigma) = S, \qquad \pi_p = 1 + \sigma\alpha, \quad \pi_q = 1 + \sigma\beta,$$
$$p = \mathrm{Norm}(\pi_p), \qquad q = \mathrm{Norm}(\pi_q).$$

makes the desired divisibility follow from the Frobenius norm formula. If p, q are prime and the chosen local curve twists have these Frobenius elements, their orders are

$$\#E(\mathbb{F}_p) = \mathrm{Norm}(\pi_p - 1) = S\,\mathrm{Norm}(\alpha), \qquad \#E(\mathbb{F}_q) = S\,\mathrm{Norm}(\beta).$$

Thus both curves have the required common order divisor, while the choice of α and β determines the remaining cofactors. Taking them as products of Gaussian factors with selected norms gives control over those cofactors, although the certificate does not require them to be smooth. Verification needs neither these cofactors nor the factors p, q themselves. The reconstruction developed below shows how the public common order can nevertheless reveal the factorization.

In this construction, p, q are outputs of the search. We do not establish an efficient way to construct a certificate for arbitrary prescribed factors, even without requiring factorization hiding. The criterion also restricts which inputs can admit a certificate: the soundness proof requires $\min(p, q) > N^{1/3}$.

2.2 Factorization Hiding

Definition 3 (Factorization Hiding). *Let* $\mathsf{Gen}(1^\kappa)$ *output a semiprime* N *and an accepting public certificate* $\mathcal{C}$*, with lengths polynomial in the security parameter* κ*. The family is factorization hiding if, for every probabilistic polynomial-time algorithm* $\mathcal{A}$*,*

$$\Pr\big[1 < d < N \ \wedge \ d \mid N : (N, \mathcal{C}) \leftarrow \mathsf{Gen}(1^\kappa),\ d \leftarrow \mathcal{A}(N, \mathcal{C})\big]$$

is negligible in κ, meaning smaller than the reciprocal of every positive polynomial for sufficiently large κ.

This definition requires that the moduli produced by Gen be hard to factor even when the certificate is withheld, and remain hard to factor when it is published. Neither follows from soundness.

For certification of an existing modulus, Gen can be viewed as a two-stage procedure: sample the private factors p, q from the intended input distribution, then run $\mathsf{Cert}(p, q; r)$ to produce a certificate $\mathcal{C}$ for $N = pq$, using randomness r. A security analysis must specify which inputs the certifier can handle and account for its probability of failure. If a construction instead chooses S first and searches for compatible factors, its security must be assessed for the moduli that search actually produces.

Our polynomial-time recovery results rule out factorization hiding for the covered families, regardless of how their certificates were generated. For a future construction outside this scope, the concrete security question is whether publishing its certificate enables a factoring attack cheaper than the General Number Field Sieve (GNFS) on the same N. Section 9 discusses this benchmark for the open construction problem.

3 Reconstruction from the Common Subgroup Order

We now develop the factor-recovery algorithm from the common subgroup order. After introducing the algebraic setup, we state the main theorem and derive the algorithm in its proof. We then examine the consequences of the result and its relation to earlier algorithms.

3.1 Quadratic Integers and Ideal Lattices

Let $K = \mathbb{Q}(\sqrt{D})$ for a negative fundamental discriminant D. We use the integral basis

$$\mathcal{O}_K = \mathbb{Z}[\omega], \quad \omega = (\nu + \sqrt{D})/2, \quad \nu \in \{0, 1\}, \quad m = (\nu^2 - D)/4.$$

Here $\nu \equiv D \pmod 2$, and the norm in these coordinates is $\mathrm{Norm}(a + b\omega) = a^2 + \nu ab + mb^2$. Conjugation replaces $\sqrt{D}$ by $-\sqrt{D}$, giving $\overline{\omega} = \nu - \omega$ and $\mathrm{Norm}(\alpha) = \alpha\overline{\alpha} = |\alpha|^2$ in the complex embedding. This identity lets us use complex lengths to bound elements with a prescribed norm.

We express the subgroup constraints as congruences modulo ideals. A nonzero integral ideal $I \subseteq \mathcal{O}_K$ is an additive subgroup closed under multiplication by $\mathcal{O}_K$, with norm given by the finite index $\mathrm{Norm}(I) = [\mathcal{O}_K : I]$. In particular, the principal ideal (α) consists of all multiples of α and has norm $\mathrm{Norm}(\alpha)$ for nonzero α. The congruence $x \equiv y \pmod I$ then means that $x - y \in I$.

In the complex embedding, each nonzero ideal is also a lattice: the integer span of two independent vectors in the plane. Translating it by an element gives an affine lattice, or coset $w + I$. The proof also uses additive lattices that need

not be ideals. For an ideal lattice, the covolume, or area of a fundamental parallelogram, is $\sqrt{|D|}\,\mathrm{Norm}(I)/2$. To control the geometry, we use Gauss reduction, which finds a basis e, f with $|e| \le |f|$ and $|\langle e, f\rangle| \le |e|^2/2$, where the brackets denote the Euclidean inner product. The sine of the angle between the basis vectors is therefore at least $\sqrt{3}/2$, a bound we will use to limit the number of candidates in the reconstruction. These quadratic-ring and lattice operations are standard; see [9,7]. All reductions below use the exact norm form.

3.2 The Reconstruction Theorem

Theorem 2 (Factoring from a Common CM Subgroup Order). *Let $N = pq$ for distinct primes $p, q > 3$, let S be prime with $\gcd(S, 2DN) = 1$, and suppose*

$$S > (N^{1/6} + 1)^2.$$

At each $\ell \in \{p, q\}$, assume one of the following:

1. *there is a Frobenius element $\pi_\ell \in \mathcal{O}_K$ of norm ℓ with $S \mid \mathrm{Norm}(\pi_\ell - 1)$;*
2. *$S \mid \ell + 1$.*

Then N can be factored from (N, S, D) in expected time polynomial in $\log N + \log S + \log |D|$. When both factors satisfy the first alternative, at most six candidate Frobenius products and 25 sums per product suffice. The alternatives need not be identified in advance.

The two alternatives describe the curve-order information supplied by the certificate. For an ordinary CM reduction, the first is precisely $S \mid \#E(\mathbb{F}_\ell)$ with Frobenius in the specified field. This does not require a maximal endomorphism ring: a nonmaximal order is still contained in $\mathcal{O}_K$, where the reconstruction takes place. A supersingular reduction has order $\ell + 1$ and satisfies the second alternative. Thus the curves and points can establish the theorem's premises even though their coordinates are not needed for recovery.

Proof. We first record the size bounds that make the reconstruction possible. In either alternative, $S \le (\sqrt{\ell} + 1)^2$, so the size hypothesis gives

$$N^{1/3} < p, q < N^{2/3}, \qquad \mathrm{Norm}(\pi_\ell - 1) < S^2$$

whenever the Frobenius occurs; the latter inequality follows from $\sqrt{\ell} + 1 < N^{1/3} + 1 < S$. In particular, $S^3 > N$.

Before constructing the lattice, consider the case where D is a nonsquare modulo S. The defining quadratic is irreducible modulo S, so $\mathcal{O}_K/S\mathcal{O}_K$ is a field. In this field, a zero norm means that the product of an element and its conjugate vanishes, so the element itself must vanish. The condition $S \mid \mathrm{Norm}(\pi_\ell - 1)$ would therefore imply $\pi_\ell - 1 \in S\mathcal{O}_K$, making its norm divisible by S^2 and contradicting the bound above. Only the second alternative can occur in this case, which we handle below.

Otherwise, choose $\lambda^2 = D \pmod S$ and define

$$u = (\nu + \lambda)/2 \pmod S, \qquad \mathcal{S} = (S, \omega - u).$$

The ideal is the kernel of the evaluation map $\omega \mapsto u$ into $\mathbb{F}_S$, so it has norm S. Its conjugate is distinct because $S \nmid D$. Whenever the first alternative occurs, $\pi_\ell - 1$ belongs to one of these two ideals. We may therefore replace π_ℓ by its conjugate to arrange $\pi_\ell \equiv 1 \pmod{\mathcal{S}}$ without changing its norm or trace. Making this choice independently at the two factors puts their Frobenius elements in the same congruence class for the argument below.

Two Ordinary Factors. We begin by reconstructing the product $Z = \pi_p \pi_q = a + b\omega$. It satisfies $\mathrm{Norm}(Z) = N$ and $Z \equiv 1 \pmod{\mathcal{S}}$. Under evaluation at $\omega = u$, Z maps to one and $\overline{Z}$ maps to N modulo S, because $Z\overline{Z} = N$. Expressed in coordinates, these relations become $a + bu \equiv 1$ and $a + b(\nu - u) \equiv N \pmod S$. Subtracting gives $b(2u - \nu) \equiv 1 - N$; here $2u - \nu \equiv \lambda$. Consequently

$$b \equiv b_0 = (1 - N)\lambda^{-1}, \qquad a \equiv a_0 = 1 - ub_0 \pmod S. \tag{2}$$

These residues determine the coordinates modulo S. To obtain a further constraint, choose integer representatives a_0, b_0 and write $a = a_0 + Sx$, $b = b_0 + Sy$. Substituting into the norm equation and reducing modulo S^2 gives

$$(2a_0 + \nu b_0)x + (\nu a_0 + 2mb_0)y \equiv \frac{N - \mathrm{Norm}(a_0 + b_0\omega)}{S} \pmod S. \tag{3}$$

The quotient on the right is integral by (2). Moreover, the two coefficients on the left cannot both vanish: their matrix has determinant $4m - \nu^2 = -D \neq 0 \pmod S$, whereas $a_0 + b_0 u = 1 \pmod S$. The congruences therefore define an explicitly computable affine lattice $w + L \subset \mathcal{O}_K$ containing the possible products, with coordinate index $[\mathcal{O}_K : L] = S^3$. Indeed, the two residues modulo S contribute an index S^2, and the nonzero linear condition on (x, y) contributes a further factor S.

It remains to find the points in this lattice whose norm equals the modulus. In the complex embedding, L has covolume $A_L = \sqrt{|D|}S^3/2$. For a Gauss-reduced basis e, f, the angle bound gives

$$|e|^2 \leq \frac{2A_L}{\sqrt{3}}, \qquad \frac{A_L}{|e|} \geq \sqrt{\frac{\sqrt{3}A_L}{2}} \geq \frac{\sqrt{3}}{2}\sqrt{S^3} > \frac{\sqrt{3}}{2}\sqrt{N}.$$

Thus the points of $w + L$ lie on parallel lines $w + jf + \mathbb{R}e$ with the spacing bounded below as in the display. The norm condition restricts the product to a circle of radius $\sqrt{N}$. This circle meets at most three of the lines, since the allowed interval of line indices has length less than $4/\sqrt{3} < 3$. Each line contains at most two points of norm N, leaving at most six candidates for Z.

To enumerate these candidates using exact arithmetic, let det denote the determinant of integer coordinates in the basis $(1, \omega)$, rather than Euclidean

area. Choose the orientation so that $\det(e, f) = S^3 > 0$ and put $c = \det(e, w)$. The indices of the lines that can meet the circle satisfy

$$|c + jS^3| \leq \left\lfloor \sqrt{\frac{4N \operatorname{Norm}(e)}{|D|}} \right\rfloor.$$

For each of these at most three integer values, substituting $w + jf + ke$ into the norm equation gives a quadratic in the integer k. Its solutions can be found with integer square and divisibility tests, so this step recovers every candidate product exactly.

Once a candidate product is fixed, the next step is to recover the sum $C = \pi_p + \pi_q$. It satisfies

$$C \equiv Z + 1 \pmod{\mathcal{S}^2}, \qquad |C| \leq \sqrt{p} + \sqrt{q} < 2S. \tag{4}$$

The congruence follows by expanding $(\pi_p - 1)(\pi_q - 1)$, whose two factors both belong to the chosen prime ideal. To work modulo its square, Hensel lifting extends the simple root u uniquely to a root u_{S^2} modulo S^2. This gives the representation $\mathcal{S}^2 = (S^2, \omega - u_{S^2})$, since the derivative $2u - \nu = \lambda \pmod{S}$ is invertible.

Choose a Gauss-reduced basis e', f' of this ideal. Rounding the basis coefficients of $Z+1$ gives a representative C_0 of its coset with coefficients in $[-1/2, 1/2]$. We can bound the distance to the true sum because every nonzero element of $\mathcal{S}^2$ has norm divisible by S^2, and hence $|e'|, |f'| \geq S$. Together with the angle bound $\sqrt{3}/2$, this shows that the basis coefficients of the true C have absolute value less than $4/\sqrt{3}$. Their differences from the coefficients of C_0 are integers of absolute value less than $4/\sqrt{3} + 1/2 < 3$. The true sum must therefore occur among

$$C = C_0 + ie' + jf', \qquad i, j \in \{-2, -1, 0, 1, 2\}.$$

For each of these 25 candidates, solve $T^2 - CT + Z = 0$ in K and retain integral roots whose norms exceed one and have product N. For the true product and sum, the root norms give the factors. The square test is exact. Write $W = C^2 - 4Z = u + v\sqrt{D}$ with $u, v \in \mathbb{Q}$. A square root $a + b\sqrt{D}$ in K must satisfy

$$h^2 = u^2 - Dv^2, \quad h \geq 0, \qquad a^2 = (h + u)/2, \quad b^2 = (u - h)/(2D), \quad 2ab = v.$$

Test these rational squares by integer square tests on reduced numerators and denominators, choose the signs using $2ab = v$, and verify by squaring. Finally require the roots $(C \pm \sqrt{W})/2$ to have integer coordinates in $(1, \omega)$.

One Ordinary and One Supersingular Factor. Now suppose the first alternative holds at p and the second at q. The second gives $q \equiv -1 \pmod{S}$, and hence $p \equiv -N \pmod{S}$. Writing the oriented Frobenius as $\pi_p = a + b\omega$, its two evaluations give

$$a + bu \equiv 1, \qquad a + b(\nu - u) \equiv -N \pmod{S}.$$

Hence

$$b \equiv (1+N)\lambda^{-1}, \qquad a \equiv 1 - bu \pmod{S}. \tag{5}$$

Since $|\pi_p| = \sqrt{p} < N^{1/3} < S$ and $|D| \geq 3$,

$$|b| < \frac{2S}{\sqrt{|D|}} \leq \frac{2S}{\sqrt{3}}, \qquad |a| < S + \frac{S}{\sqrt{|D|}} \leq (1 + 1/\sqrt{3})S.$$

These bounds let us enumerate the possible coordinates directly. Starting from the least nonnegative residues in (5), add iS, jS with $i, j \in \{-2, -1, 0, 1, 2\}$. The true pair is among these 25 choices, so testing their norms for a proper divisor of N recovers a factor.

Two Supersingular Factors. When both factors satisfy the second alternative, $S \mid p+1, q+1$. Expanding the product of these two multiples gives

$$p + q \equiv -N - 1 \pmod{S^2}, \qquad 0 < p + q < 2S^2.$$

The bound leaves only two lifts of the residue to test. The true sum is identified by the square discriminant $(p+q)^2 - 4N$, which then gives the factors. This common-order congruence is classical; see [13, Section 5].

The algorithm can try each applicable branch and check every returned divisor, so it need not identify the reduction types in advance. All lattice operations take place in dimension two using the exact quadratic norm form. These operations, the root and divisibility tests, and the constant number of candidate checks have bit complexity polynomial in the stated input lengths. Finding a square root modulo the prime S takes expected polynomial time, giving the claimed running time for the full reconstruction.

For Gaussian CM curves, the theorem continues to apply when private isogenies change the endomorphism orders. An isogeny is a nonconstant algebraic group homomorphism between elliptic curves. Curves related by an isogeny over the same finite field have the same Frobenius trace and group order, although their endomorphism orders may differ [28, Sections 2.7 and 2.11]. Their ordinary Frobenius elements therefore remain in $\mathbb{Z}[i]$, preserving the arithmetic used by reconstruction even when the original Gaussian model and its map remain private.

Corollary 1 (Prime-Order Gaussian Certificates). *Any valid prime-order certificate on* $y^2 = x^3 + Ax$ *with* $\gcd(6A, N) = 1$ *permits expected polynomial-time factorization from* (N, S) *alone.*

Proof. Soundness gives distinct factors greater than three. If $\gcd(S, N)$ is proper, it already gives a factor. Otherwise, the theorem applies with $D = -4$: the ordinary Frobenius elements belong to $\mathbb{Z}[i]$, while the supersingular curve orders are $\ell + 1$.

Prior Algorithmic Implications. The certificate congruences also connect the reconstruction to prior divisor-finding algorithms. In the Gaussian case with two ordinary reductions, the residue $r = a_0 + b_0 i \bmod S$ in (2) is a unit modulo S, since $\mathrm{Norm}(r) = N \bmod S$ and $\gcd(N, S) = 1$. Hales's algorithm [15, Theorem 1.1], which extends Lenstra's residue-divisor method [20], lists divisors Z of the Gaussian integer N satisfying $Z \equiv r \bmod S$. The required size condition, $S^3 > |N| = N$, holds here, so this call produces candidates for the Frobenius product. Retaining those of norm N includes the true product.

For each retained product, a second call uses ambient element Z, modulus $\sigma = \gcd(S, i - u)$, where $u^2 = -1 \bmod S$, and residue one. For the true product, the bound $|\sigma|^3 = S^{3/2} > \sqrt{N} = |Z|$ ensures that the call lists the Frobenius elements, whose norms factor N. Thus deriving the residue from the certificate is enough to obtain polynomial-time recovery through Hales's algorithm. For arbitrary fundamental D, a reduction to Cohn–Heninger [8, Theorem 1.3 of the full version] gives the same asymptotic conclusion; Appendix A provides the details. The proof above gives a direct alternative, enumerating at most six products in dimension two and completing each with an explicit search over 25 sums.

Broadhurst's Modulus. Broadhurst's certificate [4] supplies a prime-order point on a Gaussian curve while withholding the order cofactor. Norm reconstruction factors its 5061-digit modulus from N, S alone; Section 8 reports the computation. Section 5 proves the alternative public-point method.

4 Factoring by Quadratic Twists

A public curve-order multiple can enable factoring even when its prime factorization is unknown. We recall the quadratic-twist method of [23,13] and apply it to Reble's certificate. This illustrates full-order disclosure alongside the common-order disclosure treated above.

Let $N = pq$ and write $n_p = \#E(\mathbb{F}_p)$, $n_q = \#E(\mathbb{F}_q)$. Suppose a public integer k is divisible by both n_p and n_q. Multiplication by k sends every point on E to the identity at both primes. Choose a unit c with Jacobi symbol $(c/N) = -1$ and consider

$$E^{(c)} : y^2 = x^3 + c^2 Ax + c^3 B.$$

The twist is isomorphic to E at one prime and is a nontrivial quadratic twist at the other, where its order is $2(\ell+1) - n_\ell$: the Jacobi symbol is the product of the two local quadratic characters, so exactly one sees a nonsquare twist parameter. Such a twist negates the Frobenius trace, changing $\ell + 1 - t_\ell$ to $\ell + 1 + t_\ell$. Thus k annihilates the first component. If it leaves the second nonzero, the projective denominator of the result vanishes at exactly one prime, and its GCD with N returns a factor. Projective x-coordinate arithmetic performs this test without computing a square root to obtain a full point.

The effectiveness of the x-only test depends on the groups of points on the nontrivial quadratic twists. The following count makes that dependence explicit.

It concerns valid projective multiplication, including the identity and exceptional coordinate cases. Any nonunit denominator encountered during arithmetic can itself expose a factor.

Proposition 1 (Twist Separation Probability). *Let $p, q \geq 23$ be distinct primes such that E is nonsingular modulo both, and let k be a positive integer annihilating both $E(\mathbb{F}_p)$ and $E(\mathbb{F}_q)$. For $\ell = p, q$, let H_ℓ be the group of points on the nontrivial quadratic twist of E over $\mathbb{F}_\ell$, write $H_\ell[k] = \{R \in H_\ell : [k]R = \mathcal{O}\}$ for its subgroup annihilated by k, and put*

$$b_\ell = \frac{|H_\ell| - |H_\ell[k]|}{2\ell}.$$

For uniformly random $x \bmod N$, the probability that x-only multiplication by k gives the identity at exactly one prime is

$$b_p(1 - b_q) + (1 - b_p)b_q. \tag{6}$$

It is zero exactly when k annihilates both H_p and H_q; otherwise it is at least $1/8$.

Proof. At a fixed prime, each affine x lies on the curve or its quadratic twist. The two points above a non-root of the cubic are negatives of each other. The local 2-torsion is shared by the two groups and is annihilated by k, since it corresponds under twisting to rational 2-torsion on $E(\mathbb{F}_\ell)$. Thus exactly $(|H_\ell| - |H_\ell[k]|)/2$ affine x-coordinates survive multiplication. The Chinese remainder theorem makes the two local choices independent, giving (6).

If $H_\ell[k]$ is proper, its order is at most $|H_\ell|/2$. For $\ell \geq 23$, Hasse's bound gives $\ell/2 \leq |H_\ell| \leq 3\ell/2$. Consequently $0 \leq b_\ell \leq 3/4$, and a positive b_ℓ is at least $1/8$. The minimum of (6) on these ranges, with at least one positive b_ℓ, is at least $1/8$.

Small prime factors can be removed by trial division. The annihilation condition itself need not be decidable from the public input. In particular, a trace-zero curve and its quadratic twist both have order $\ell + 1$. If both local traces are zero, the test always fails for every k divisible by both curve orders. Factoring then requires another method, such as the common-order reconstruction of Section 3 when its hypotheses hold.

Reble's Modulus. Reble's public certificate [24] includes N, A, s, t, Z with

$$E : y^2 = x^3 + Ax, \qquad [2st]Z = \mathcal{O}, \qquad Q = [2t]Z, \qquad [s]Q = \mathcal{O}.$$

Certificate validity also requires Q to be nonzero at both primes. For the recovered factors, the local curve orders are $n_p = 2st_p$, $n_q = 2st_q$, with $t = t_p t_q$. Consequently $k = 4st$ is divisible by both orders. The quadratic-twist test using the public integers N, A, s, t recovers the factors of this 1084-digit modulus; the exact product verifies the result.

5 Public-Point Methods and Composite Orders

The public point reveals a CM orientation that can simplify recovery. We first treat prime orders on Gaussian curves and in other CM fields, then extend the Gaussian method to factored composite orders, for which no individual prime divisor need reach the soundness threshold.

5.1 Recovery from a Gaussian Point

For Gaussian curves, the public-point method gives the following result.

Theorem 3 (Factoring from a Gaussian Certificate). *Let N be composite and nonsquare, let $\gcd(6A, N) = 1$, and let $P \in E(\mathbb{Z}_N)$ be an affine point on $E : y^2 = x^3 + Ax$. Suppose S is prime, $S > (N^{1/6}+1)^2$, and $[S]P = \mathcal{O}$. Then $N = pq$ for distinct primes $p, q > 3$, and its factorization can be recovered in expected time polynomial in $\log N + \log S$ from (N, S, A, P). In the ordinary/ordinary branch, four Gaussian unit choices and at most 25 candidate sums suffice. If a square root of -1 modulo S is supplied, that branch is deterministic.*

Proof. Soundness gives $N = pq$ and $N^{1/3} < p, q < N^{2/3}$. First test $\gcd(S, N)$, which gives a factor if nontrivial. For $\ell = p, q$, Hasse's bound gives $\#E(\mathbb{F}_\ell) < S^2$, so the rational S-torsion is generated by P_ℓ. At an ordinary factor $\ell \equiv 1 \pmod 4$, the automorphism $(x, y) \mapsto (-x, uy)$, $u^2 = -1$, therefore acts on P_ℓ by a scalar whose square is $-1 \bmod S$. Thus an ordinary factor forces $S \equiv 1 \pmod 4$.

In this case find $\lambda^2 = -1 \bmod S$, put $Q = [\lambda]P$, and compute $d = \gcd(x_Q + x_P, N)$. Proper arithmetic GCDs already give factors. At an ordinary factor $x_Q = -x_P$; at a supersingular factor $\ell \equiv 3 \pmod 4$ this equality would give $(y_Q/y_P)^2 = -1$, which is impossible. Here y_P is a unit because P has odd order. Consequently a proper d factors N, while $d = N$ gives $r = y_Q/y_P$ with $r^2 = -1 \bmod N$.

In the latter branch, identify i with $\iota(x, y) = (-x, ry)$, so that $\iota(P) = [\lambda]P$. The Gaussian GCDs

$$\sigma = \gcd_{\mathbb{Z}[i]}(S, \lambda - i), \qquad Z_0 = \gcd_{\mathbb{Z}[i]}(N, r - i)$$

generate the kernels of evaluation at $i = \lambda \bmod S$ and $i = r \bmod N$, so have norms S and N. Frobenius fixes P_ℓ, so $\pi_\ell \equiv 1 \pmod \sigma$. On the invariant differential, ι acts by $-1/r = r$; the zero differential of Frobenius therefore gives $\pi_\ell(i = r) = 0 \bmod \ell$. The ideal (π_ℓ) has norm ℓ and is thus the local evaluation kernel. Chinese remaindering gives $(Z_0) = (\pi_p \pi_q)$. The four Gaussian units have distinct images modulo σ, so exactly one unit multiple satisfies $Z \equiv 1 \pmod \sigma$. For $C = \pi_p + \pi_q$,

$$C \equiv Z + 1 \pmod{\sigma^2}, \qquad |C| < 2N^{1/3} < 2S.$$

Nearest-coordinate reduction modulo σ^2 therefore leaves 25 lifts, as in Section 3. Solving $T^2 - CT + Z = 0$ in $\mathbb{Z}[i]$ and checking the root norms recovers p, q.

If $d = 1$, or if $S \equiv 3 \pmod 4$, both factors are supersingular. Then $p + q \equiv -N - 1 \pmod{S^2}$ and $0 < p + q < 2S^2$ leave two integer sums to test by their discriminants. All steps have polynomial bit complexity; only finding λ requires randomness.

Appendix B gives an optional public test that reduces the sum search to a single lift.

5.2 Other CM Fields

The Gaussian method uses the public point to select a CM orientation at both prime factors. The same argument works in other imaginary quadratic fields when a suitable CM map can be evaluated publicly. We explain the additional hypotheses and the ideal reconstruction; the final sum search is the one proved in Section 3.

Consider a prime-order certificate (N, S, E, P) with $S > (N^{1/6} + 1)^2$, where $E : y^2 = x^3 + Ax + B$ and $P = (X, Y)$. Use K, D, ω, ν as in Section 3, and assume $\gcd(N, 6D) = \gcd(S, 2DN) = 1$. Suppose the local curves are nonsingular reductions of curves with CM by the maximal order $\mathcal{O}_K$. At a prime that splits in K, the reduction is ordinary and its Frobenius belongs to $\mathcal{O}_K$. At an inert prime ℓ, meaning that the prime remains prime in $\mathcal{O}_K$, the reduction is supersingular with order $\ell + 1$.

The extra public input is a rational function $f(x)$ giving the map

$$\psi(x, y) = \left(f(x), \frac{y f'(x)}{\sqrt{D}} \right), \qquad \psi^2 = [D], \tag{7}$$

defined after adjoining $\sqrt{D}$, with differential $\sqrt{D}$. Its coefficient denominators must be units, and its homogeneous numerator and denominator must have no common zero over the algebraic closure of either residue field. These conditions ensure that the displayed formulas specialize to the intended map. Since $S \nmid D$, the image of each local point has odd order S, so it is affine with nonzero y-coordinate. Consequently $f(X)$ is finite and $Y f'(X)$ is a unit, justifying the divisions below.

Recovering the Orientation. Soundness and Hasse's bound give $N = pq$ and one-dimensional rational S-torsion at each factor, as in the Gaussian proof. At an ordinary factor, ψ is defined over the residue field and acts on this torsion by a scalar whose square is $D \bmod S$. If no such scalar exists, both reductions are supersingular and the preceding two-sum reconstruction applies.

Otherwise choose $\lambda^2 = D \bmod S$, set $Q = [\lambda]P$, and compute $d = \gcd(x_Q - f(X), N)$. At an ordinary factor, Q is either $\psi(P)$ or $-\psi(P)$, so its x-coordinate is $f(X)$. At an inert factor, that equality would make $Y f'(X)/y_Q$ a square root of D, which is impossible there. Thus a proper d factors N, while $d = 1$ again gives two supersingular reductions. As usual, a proper GCD encountered during point arithmetic already supplies a factor.

It remains to handle $d = N$, when both reductions are ordinary. The map identity gives

$$r = Y f'(X) y_Q^{-1} \pmod N, \qquad r^2 = D \pmod N.$$

Using this r for $\sqrt{D}$ makes $\psi(P) = [\lambda]P$ at both factors. Thus the point aligns the differential and torsion orientations. Here r and λ represent $\sqrt{D}$; in the Gaussian proof they represented i.

Recovering the Frobenius Product. Put

$$u_N = (\nu + r)/2 \pmod N, \qquad u_S = (\nu + \lambda)/2 \pmod S,$$
$$J = (N, \omega - u_N), \qquad \mathcal{S} = (S, \omega - u_S).$$

For the oriented Frobenius $\pi_\ell = a + b\omega$, the identity $2\pi_\ell = [2a + \nu b] + [b]\psi$ connects these evaluations to its action on the curve. Its zero differential gives $a + bu_N = 0 \bmod \ell$, while its action fixing P_ℓ gives $a + bu_S = 1 \bmod S$. The first congruence identifies (π_ℓ) with the evaluation kernel of norm ℓ. Chinese remaindering and the second congruence therefore give

$$J = (\pi_p \pi_q), \qquad \pi_p, \pi_q \equiv 1 \pmod{\mathcal{S}}.$$

In particular, J is principal even when K has nontrivial class group. Its public basis $N, \omega - u_N$ allows us to recover a generator by Gauss reduction. Indeed, writing $Z = \pi_p \pi_q$, every nonzero element of J has the form $Z\alpha$ with $\alpha \in \mathcal{O}_K$ and satisfies

$$|Z\alpha|^2 = N \operatorname{Norm}(\alpha) \geq N.$$

Equality holds precisely when α is a unit, so a shortest vector determines Z up to a unit. Among the at most six choices, the true product is selected by $Z \equiv 1 \pmod{\mathcal{S}}$; the units have distinct images modulo $\mathcal{S}$ because $S > 3$.

The sum $C = \pi_p + \pi_q$ now satisfies $C \equiv Z + 1 \pmod{\mathcal{S}^2}$ and $|C| < 2S$. The ideal-square construction, 25-lift search, and exact quadratic square test in Section 3 recover its two summands, whose norms factor N. The reconstruction takes expected time polynomial in $\log N + \log S + \log |D|$, for arbitrary class number, apart from obtaining and evaluating the specified map.

Appendix C supplies the maps used in the experiments. The map for $\sqrt{D}$ has degree $|D|$, so its explicit representation can grow beyond polynomial size in $\log |D|$. The norm-lattice method of Theorem 2 recovers the product directly from (N, S, D) and avoids this map cost.

5.3 Composite Point Orders

On Gaussian curves, a sufficiently large point order with known prime factorization also permits recovery. The local curve orders may retain unknown cofactors. For a certificate of Definition 2, summing the certified points gives the required point of product order.

Theorem 4 (Gaussian Certificates with Factored Point Orders). *Let N be composite and nonsquare, let $\gcd(6A, N) = 1$, and let $P \in E(\mathbb{Z}_N)$ for $E : y^2 = x^3 + Ax$ be affine. Suppose an integer $M = \prod s^{e_s}$ is supplied with its certified prime factorization, $[M]P = \mathcal{O}$, and $[M/s]P$ is strongly nonzero for every $s \mid M$. If $M > (N^{1/6} + 1)^2$, then N can be factored in expected polynomial time in the public input length. This also covers the certificates of Definition 2 on this Gaussian curve.*

Proof. The hypotheses give P exact order M at every prime divisor. Soundness and Hasse's bound give $N = pq$, $N^{1/3} < p, q < N^{2/3}$, $\#E(\mathbb{F}_\ell) < M^2$, and $N < M^3$. Trial division handles $M < 16$, so assume $M \geq 16$. Throughout, a point becoming the identity at only one factor exposes it through a denominator GCD; a point nonidentity at both factors has affine coordinates. We also test $\gcd(M, N)$, which is proper if nontrivial because Hasse's bound at the smaller factor gives $M < N$.

Finding a square root or a factor. In $\mathbb{Z}[i] = \mathbb{Z}[i]$, primes $s \equiv 1 \pmod 4$ split into conjugate factors, primes $s \equiv 3 \pmod 4$ are *inert*, meaning that (s) remains prime, and $(2) = (1 + i)^2$ up to a unit. The curve is ordinary at $\ell \equiv 1 \pmod 4$ and supersingular with group order $\ell + 1$ at $\ell \equiv 3 \pmod 4$.

For each $s \equiv 1 \pmod 4$ dividing M, find $\lambda_s^2 = -1 \bmod s$, set $T = [M/s]P$, and compute $Q = [\lambda_s]T$ and $d_s = \gcd(x_Q + x_T, N)$. A proper d_s factors N; if $d_s = N$, the curve equation gives $r = y_Q/y_T$ with $r^2 = -1 \bmod N$. The denominator is a unit because T has odd order. This equality is impossible at an inert prime divisor of N, where -1 has no square root.

Suppose all $d_s = 1$. At an ordinary factor, T then has nonzero components in both eigenspaces of i, whose eigenvalues are $\pm\lambda_s$. Thus $[M/s^{e_s}]P$ has order s^{e_s} in each component, generating a Gaussian module of size s^{2e_s}. For an inert order prime s, its annihilator is (s^{e_s}), also of norm s^{2e_s}. A component of order 2^e has annihilator $(1+i)^a$, where $a = 2e-1$ or $2e$, since the least power of two in this ideal is $2^{\lceil a/2 \rceil}$. Multiplying these sizes gives $\#E(\mathbb{F}_\ell) \geq M^2/2$, and Hasse's bound implies $\ell > M^2/4$.

Both factors cannot be ordinary, since then $N > M^4/16 \geq M^3$. In the mixed case, the supersingular factor $v < 4M$ satisfies $M \mid v + 1$, so testing $\gcd(kM - 1, N)$ for $1 \leq k \leq 4$ finds it; the ordinary factor exceeds $M^2/4 \geq 4M$. If both factors are supersingular,

$$p + q \equiv -N - 1 \pmod{M^2}, \qquad 0 < p + q < 2M^2.$$

The two possible sums are tested by their discriminants. Running both searches therefore factors N whenever the preceding tests fail to supply r.

Computing the common annihilator. A root r makes both factors ordinary and defines $\iota(x, y) = (-x, ry)$. For $\ell = p, q$, put

$$I_\ell = \mathrm{Ann}_{\mathbb{Z}[i]}(P_\ell) := \{a + bi \in \mathbb{Z}[i] : [a]P_\ell + [b]\iota(P_\ell) = \mathcal{O}\}.$$

Here Ann denotes the annihilator ideal, consisting of the scalars that send the point to the identity. Since $\mathbb{Z}[i]/I_\ell \simeq \mathbb{Z}[i]P_\ell$, its norm is the size of the generated module, at least M.

For each split order prime s, lift λ_s to a root modulo s^{e_s} and form

$$U = [M/s^{e_s}]P, \qquad V_+ = \iota(U) + [\lambda_s]U, \qquad V_- = \iota(U) - [\lambda_s]U.$$

These maps isolate the two eigenspaces, acting there by the units $\pm 2\lambda_s$. Repeated multiplication by s gives their orders s^a, s^b. Different stopping steps at the two factors expose a denominator GCD; otherwise both annihilators have the same factor $(\sigma_s)^a(\bar{\sigma}_s)^b$, where $(\sigma_s) = (s, i - \lambda_s)$ is computed by a Gaussian GCD.

Each inert order prime contributes (s^{e_s}). For $2^e \| M$, apply $1 + \iota$ repeatedly to $[M/2^e]P$; the first identity gives the exponent of $(1 + i)$. Different stopping steps again factor N. Otherwise, multiplying these factors gives

$$I_p = I_q = (\tau), \qquad \mathrm{Norm}(\tau) \geq M.$$

Reconstructing Frobenius. Frobenius fixes the generated modules, so $\pi_p, \pi_q \equiv 1 \pmod{\tau}$. As in Theorem 3, a generator of $(N, r - i)$ gives $Z = \pi_p \pi_q$ up to a unit. Try its four unit multiples, retaining those congruent to 1 modulo τ. The true product is included, and its sum satisfies

$$C = \pi_p + \pi_q \equiv Z + 1 \pmod{\tau^2}, \qquad |C| < 2N^{1/3} < 2M \leq 2|\tau^2|.$$

Nearest-coordinate reduction of $Z + 1$ modulo τ^2 gives C_0, leaving the 25 candidates $C = C_0 + (a + bi)\tau^2$ with $a, b \in \{-2, -1, 0, 1, 2\}$. For each, solve $T^2 - CT + Z = 0$ in $\mathbb{Z}[i]$ and test whether the root norms are nontrivial factors with product N.

The number of order tests is polynomial in $\log M$. Gaussian GCDs, lifting, and exact quadratic-root tests have polynomial bit complexity; finding the modular roots takes expected polynomial time. Finally, summing certificate points of pairwise coprime orders gives their product order at both factors, so the algorithm applies to the multiple-point certificate as well.

For the CM torsion structure used here, see [26, Chapter II, Proposition 1.4(b) and the proof of Proposition 4.4]. Appendix D.8 illustrates the reconstruction with noncyclic rational torsion and small prime powers.

6 Constructing Certificates with Private Cofactors

Constructing a certificate requires compatible local curves, while factorization hiding requires that their public parameters resist the recovery methods above. We examine these constraints before describing a controlled construction based on private isogeny descent.

Local Orders and CM Parameters. For fixed, privately known factors p, q, the local curves must have orders

$$\#E_p(\mathbb{F}_p) = Sm_p, \qquad \#E_q(\mathbb{F}_q) = Sm_q,$$

with a common public divisor $S > (N^{1/6}+1)^2$. The cofactors m_p, m_q may differ and remain private. Bröker and Stevenhagen [5] give a CM method for constructing a curve of prescribed order while choosing the characteristic.

CM parameters can themselves reveal the factors. For a public curve $E : y^2 = x^3 + Ax + B$, good reduction makes

$$j(E) = 1728 \cdot 4A^3/(4A^3 + 27B^2)$$

computable modulo N. An imaginary quadratic order of discriminant Δ has a class polynomial $H_\Delta(T) \in \mathbb{Z}[T]$, whose roots are the j-invariants of complex curves with that endomorphism order. Its degree is the class number $h(\Delta)$; for fundamental Δ, it is the Hilbert class polynomial [9, Proposition 13.2]. If an available class polynomial vanishes at one local invariant but not the other, then

$$H_\Delta(j) = 0 \pmod{p}, \quad H_\Delta(j) \neq 0 \pmod{q} \quad \Longrightarrow \quad \gcd(H_\Delta(j), N) = p.$$

For a known shared field, Theorem 2 applies under its order and coprimality hypotheses.

Restrictions from Local Group Orders. A sufficiently large common divisor can also expose the factors without any CM information. The following bound quantifies this restriction.

Proposition 2 (Large Common Subgroups). *Let $p, q > 3$ be distinct primes and $N = pq$. Let elliptic curves over $\mathbb{F}_p, \mathbb{F}_q$ have orders aS, bS for an integer $S > 4$. Put $T = \lfloor 16N/S^2 \rfloor$. Given only N, S, one can factor N in $O(T^2)$ iterations, each with bit complexity polynomial in $\log N$. In particular, $S \geq \sqrt{N}/\operatorname{poly}(\log N)$ gives a polynomial-time attack.*

Proof. Hasse's bound implies $|\sqrt{p} - \sqrt{aS}| \leq 1$ and $|\sqrt{q} - \sqrt{bS}| \leq 1$. Multiplying these errors by $\sqrt{b}$ and $\sqrt{a}$, respectively, and applying the triangle inequality gives

$$|\sqrt{bp} - \sqrt{aq}| \leq \sqrt{b} + \sqrt{a},$$

because $\sqrt{b}\sqrt{aS} = \sqrt{a}\sqrt{bS}$. Put $k = ab$ and $v = bp + aq$. Since $a, b \geq 1$, it follows that

$$0 \leq v - \sqrt{4kN} = (\sqrt{bp} - \sqrt{aq})^2 \leq (\sqrt{a} + \sqrt{b})^2 \leq 4ab = 4k.$$

Thus, once k is fixed, the integer v lies in a short interval.

We can bound k using the same Hasse inequalities: $aS \leq 4p$ and $bS \leq 4q$ give $ab \leq 16N/S^2$, hence $k \leq T$. The algorithm therefore tries each $1 \leq k \leq T$ and, for each, the $4k+1$ integers starting at $\lceil \sqrt{4kN} \rceil$ as candidates for v. It tests whether $v^2 - 4kN$ is a square.

The true pair is included, and its square root is $d = |bp - aq|$. Then $v + d$ is either $2bp$ or $2aq$. The GCD with N is proper: $S > 4$ and Hasse's bound imply $a < p$ and $b < q$, so q cannot divide $2bp$ and p cannot divide $2aq$. Testing the candidate GCDs therefore recovers a factor. The total number of candidates is $\sum_{k=1}^{T}(4k+1) = O(T^2)$, and all quantities have $O(\log N)$ bits.

This is an application of the classical scaled difference of squares method [19].

Equal full local orders impose a stronger restriction, even if the common order is private. If both orders equal n, Hasse gives $|\sqrt{p}-\sqrt{n}| \le 1$ and $|\sqrt{q}-\sqrt{n}| \le 1$, so

$$\frac{p+q}{2} - \sqrt{N} = \frac{(\sqrt{p}-\sqrt{q})^2}{2} \le 2.$$

The midpoint $(p+q)/2$ is an integer and $\sqrt{N}$ is not. Consequently, the midpoint is either $\lceil\sqrt{N}\rceil$ or $\lceil\sqrt{N}\rceil + 1$. Ordinary Fermat factorization therefore finds the factors with at most two square tests.

Private Descent within the Gaussian Field. Private isogeny descent changes the endomorphism order while preserving the CM field and local group order. Starting from a Gaussian curve, each descending rational 2-isogeny doubles the conductor, the index of the endomorphism order in $\mathbb{Z}[i]$. A chain of k such steps reaches the order $\mathbb{Z} + 2^k\mathbb{Z}[i]$, giving a direct way to construct curves whose endomorphism orders have large conductor.

To arrange the common divisor, fix a depth $k \ge 1$, choose $\sigma \in \mathbb{Z}[i]$ of odd prime norm S, and sample $\alpha \in \mathbb{Z}[i]$ so that

$$\pi = 1 + \sigma\alpha, \qquad p = \mathrm{Norm}(\pi) > 3 \text{ is prime}, \qquad v_2(\mathrm{Im}\,\pi) = k.$$

Here v_2 is the exact exponent of two dividing the imaginary coordinate. The prime p is selected as part of the construction. A suitable Gaussian CM twist has Frobenius π and group order $\mathrm{Norm}(\pi - 1) = S\,\mathrm{Norm}(\alpha)$. Choose a point of order S on this curve and transport it along k descending rational 2-isogenies. Its order stays S, because the composite isogeny has degree 2^k, coprime to S.

Repeat at a distinct prime q, combine the final curve coefficients and points by CRT, and check the certificate size condition. Publish the combined curve and point, and retain the cofactors and isogeny paths privately. Appendix E gives the sampling procedure and explains how the descending paths are chosen in the isogeny graph, using the volcano structure of [28].

The final endomorphism order has discriminant $-4 \cdot 2^{2k}$, but its fundamental field discriminant is still -4. Norm reconstruction therefore uses the unchanged Gaussian field together with the public N, S, as in Theorem 2. Section 8 reports the generated examples and recovery measurements.

7 Implications for Elliptic-Curve Encryption

We apply the preceding methods to elliptic-curve encryption when order information is disclosed or recovered through attacks on small private exponents.

Demytko and Small-Exponent Attacks. Demytko's primitive uses x-coordinate multiplication on a curve and its local quadratic twists. The four local group orders remain private, while the public exponent is chosen coprime to all four [10, Section 4]. Nitaj–Fouotsa [22, Sections 3–4] recover products of local orders

under small-solution bounds and a zero-dimensionality assumption on the derived polynomial system. Their subsequent factor-recovery step uses smoothness and partial factor information.

Once the product k is available, the quadratic-twist method of Section 4 provides another way to complete the attack. Each local order can come from the curve or its twist. The product therefore annihilates one group at each prime. If it fails to annihilate the other group at either prime, the counting argument of Proposition 1 applies after interchanging the two groups where necessary. Random x-coordinates sample both choices, so the attack can proceed without identifying them. This gives expected polynomial-time factorization using k directly, regardless of its smoothness, under the assumptions used to recover it and the stated twist separation.

Order Disclosure in the Boudabra–Nitaj RSA Variant. Boudabra–Nitaj [3] use ephemeral curves $y^2 = x^3 + Ax$ with ordinary Gaussian reductions. Their public key is (N, e); a valid affine ciphertext determines A when its x-coordinate is invertible. Section 6.4 of the journal version assumes additionally that $k = \#E(\mathbb{F}_p)\#E(\mathbb{F}_q)$ is known and treats factoring k as an obstacle to factoring N. Section 6.5, Remark 1, invokes the same obstacle after recovering k through small-private-exponent analysis.

Under twist separation, (N, A, k) suffices to factor N without factoring k, refuting this obstacle in both sections. Our tests used their published 138-bit example and a 4096-bit instance we generated, with k supplied from the known setup in both cases (Section 8).

Adding a Public Certificate to Elliptic-Curve Paillier. Galbraith's scheme [12, Section 9] publishes (N, E, Q) with $Q \in E(\mathbb{Z}/N^2\mathbb{Z})$ and keeps an annihilator of Q private. He also suggests constructing E, p, q jointly by CM. Our application concerns the additional disclosure introduced by attaching a public semiprimality certificate to such an instance. Suppose that the key also publishes a prime $S > (N^{1/6} + 1)^2$, with the reduction of Q having exact order S at both prime factors. Under the known-field and coprimality hypotheses, Theorem 2 then factors N from this augmented public information. Section 8 reports a Gaussian instance.

When the published S also satisfies $[S]Q = \mathcal{O}$ modulo N^2 and $\gcd(S, N) = 1$, direct decryption already follows from Galbraith's own rule. A ciphertext $C = [r]Q + P_m$ satisfies

$$[S]C = P_{Sm}.$$

Here P_m is the message encoding in the kernel of reduction from $E(\mathbb{Z}/N^2\mathbb{Z})$ to $E(\mathbb{Z}_N)$. The kernel group law adds the message parameters modulo N, so reading this encoding and inverting S mod N recovers m [12, Sections 3 and 9].

Supersingular Parameters. The KMOV schemes [16, Section 5] use supersingular parameters with local orders $p+1$ and $q+1$, which remain private. Their original

analysis already relates recovery of $\mathrm{lcm}(p+1, q+1)$ to factoring [16, Theorem 8]. For the product, a disclosed $k = (p+1)(q+1)$ immediately gives

$$p + q = k - N - 1,$$

from which the factors follow. A sufficiently large public common torsion order also enables the supersingular reconstruction of [13] and Section 3.

8 Computational Results

We tested the recovery methods on Reble's and Broadhurst's certificates [24,4] and on generated certificates, then checked the lattice computations against direct enumeration. Recovery timings are individual local runs using Python with GMP integer arithmetic, excluding construction, certificate validation, and primality testing.

Every returned factorization was checked by exact multiplication. For generated certificates, the known factors were used to construct the inputs and verify the curve equation, point orders, and size conditions. Recovery received only the stated public inputs.

8.1 Reble's and Broadhurst's Certificates

Broadhurst's 5061-digit modulus factored in 7.902 seconds using the public-point method of Section 5, with input (N, S, A, P). Norm reconstruction (Section 3) from N, S alone took 0.465 seconds and returned the same factors, of 2531 and 2530 digits. Quadratic twisting factored Reble's 1084-digit modulus in 0.431 seconds using N, A, s, t, as described in Section 4. Appendix D records the factors and recovered curve orders.

We verified Broadhurst's curve and point relations, the certificate threshold, and the Gaussian norm identities. The recovered factors and order cofactors pass probable-prime tests. Broadhurst reports a Primo primality proof for S, which we have not independently revalidated; conditional on its primality, the verified certificate proves that the recovered factors are prime.

8.2 Generated Certificates

Gaussian Curves. A controlled CM construction following Section 2.1 produced a certificate with a 142-bit modulus. Public-point recovery (Section 5) took 0.0006 seconds, while norm reconstruction (Section 3) from N, S took 0.00038 seconds and returned the same factors. Appendix D gives the certificate data.

We also tested certificates obtained by transporting points along private isogeny chains. These chains change the endomorphism order while preserving the Gaussian field; Section 6 describes their construction. Norm reconstruction from Section 3 factored the 284-, 521-, and 1024-bit examples from N, S in approximately 0.0021, 0.00042, and 0.00082 seconds, respectively. The 1024-bit

instance used a 351-bit prime S, private cofactors of 165 and 160 bits, and a descent of 110 steps at each factor. Construction and validation took about 79 seconds; the endpoint parameters are recorded in Appendix E. Separate checks proved S, p, q prime and verified the Gaussian norm identities for all three. An independent implementation of Theorem 2, receiving only N, S, D, also recovered their factors and those of Broadhurst's modulus.

Other CM Fields. The public-map method of Section 5 factored eight generated certificates for $D = -3, -7, -15$, including moduli of 1019, 1017, and 1022 bits, respectively. Exact symbolic identities verified the maps used in these tests. Appendix C gives their formulas.

Private Descent in Distinct Fields. We also generated certificates whose two local curves have different CM fields, then transported their points along private isogeny chains (Appendix E.4). A 112-bit example used fields of discriminants -4 and -8, with six isogenies at each factor. The starting-field norm tests and fifteen small class-polynomial tests found no factor, but endpoint polynomials of degrees 32 and 64 recovered the factors using the class-polynomial GCD test of Section 6.

Thirty further certificates over 1000-, 2000-, and 4000-bit moduli, with descents of up to 83, 166, and 333 steps, passed validation. A degree-2048 polynomial recovered factors at depth twelve for all three modulus sizes. Computing it took about 124 seconds; for the 4000-bit modulus, coefficient reduction took 0.31 seconds and evaluation with a GCD took 0.011 seconds. The polynomials at the deepest endpoints were not computed.

Composite Point Orders. The method of Section 5.3 recovered a proper factor from each of eleven certificates over nine moduli of 22–48 bits. These tests covered split, inert, and ramified order primes, mixed and supersingular reductions, and unequal local annihilators. The local primes and order factorizations were independently certified; Appendix D.8 records the examples.

A larger instance had a 1023-bit modulus and a 349-bit point order M, the product of four 88-bit primes. Recovery took about 0.09 seconds using only N, A, P and the factorization of M. The same modulus also admitted a certificate with four separate prime-order points; adding them allowed the same recovery, confirming the multiple-point reduction.

8.3 Encryption Parameters

To test the Boudabra–Nitaj order-disclosure scenario of Section 7, we supplied the local curve-order product k from the known setup, together with N, A, to the quadratic-twist algorithm (Section 4). It factored their published 138-bit example and a 4096-bit modulus we generated. The latter took 4.26 seconds; independent checks verified the local orders and twist separation.

For the augmented elliptic-curve Paillier parameters of Section 7, we constructed a 511-bit Gaussian instance with the additional public order S and

checked the lift of Q modulo N^2. Public-point reconstruction (Section 5), applied to Q mod N, recovered the factors in 0.006 seconds.

8.4 Arithmetic Validation

The lattice enumerators of Section 3 agreed with direct coordinate enumeration in 13,030 Gaussian cases and 26,140 general-field cases. A finite grid with local primes at most 1200, subgroup primes at most 151, and 17 discriminants yielded 735 ordinary/ordinary, 371 mixed, and 119 supersingular inputs meeting the arithmetic hypotheses of Theorem 2; all factored successfully. These inputs test the algebraic reconstruction without constructing curve certificates.

For $D = -23$, an example with $S = 233$ verified norm reconstruction with nonprincipal ideals $\mathcal{S}$ and $\mathcal{S}^2$. A separate test supplied oriented roots to check the ideal-reconstruction stage of Section 5; Appendix D.7 records that example. Boundary tests covered three intersecting lattice lines, a sum offset of two, tangency, rounding ties, and 49 signed-residue cases.

9 Limits and Factoring Cost

The known-field reconstruction theorem leaves open constructions whose local curves have distinct or unrecognized CM fields. Endpoint class-polynomial attacks recover factors in some of our controlled distinct-field examples, but the deeper cases remain unresolved (Section 8). An efficient public certifier for arbitrary fixed factors also remains open.

For a future construction, the benchmark is the cost of applying the General Number Field Sieve (GNFS) to the same modulus. Its heuristic asymptotic scale is

$$\exp\Big(\big((64/9)^{1/3} + o(1)\big)(\log N)^{1/3}(\log\log N)^{2/3}\Big).$$

Our polynomial-time attacks rule out factorization hiding for their covered families.

A concrete comparison must use the modulus distribution produced by the construction and account for attack success probability, precomputation, and memory. Increasing the cost of one attack does not establish security against the others. In particular, the leading GNFS term alone does not give a reliable crossover at practical sizes [18].

10 Conclusion

For cryptographic use, a public certificate must establish that a modulus is semiprime while preserving its factoring difficulty. We formalized a semiprimality criterion derived from Goldwasser–Kilian, using a point of sufficiently large public prime order S on an elliptic curve modulo N, and generalized it to composite point orders with certified prime factorization.

For the CM families covered by Theorem 2, this same order information yields congruences on the unknown Frobenius elements that make the factors recoverable. Our reconstruction combines these congruences with the norm relations in a two-dimensional lattice, leaving only a constant number of candidate products and sums when both reductions are ordinary. The resulting algorithm factors N in expected polynomial time from (N, S, D) alone, with D identifying the known field. Using the public point gives analogous constraints for Gaussian certificates with factored composite point orders.

These reconstructions and quadratic twisting recover the factors of Reble's 1084-digit and Broadhurst's 5061-digit moduli [24,4]. Broadhurst's certificate is particularly instructive: withholding its curve-order cofactor still leaves N, S sufficient for recovery. The attack's independence from the curve model and CM map also explains why private isogeny descent within a known field leaves it applicable: descent changes the endomorphism order but preserves the Frobenius trace and group order, retaining the constraints used by norm reconstruction.

For encryption schemes in which a product of local curve orders is disclosed or recovered, the quadratic-twist analysis shows how to use it directly, subject to twist separation. This strengthens existing small-exponent attacks and corrects claims that the difficulty of factoring the order product prevents recovery of the modulus factors (Section 7).

Experiments with distinct local CM fields identify further cases in which the public curve reveals factors, while the more general possibilities remain open. The central construction question is therefore: *can one efficiently construct a public curve-and-point certificate for a fixed modulus from its privately known factors while preserving its factoring difficulty relative to the General Number Field Sieve?*

Acknowledgments. GPT-6.1 Sol was used to assist with proof analysis, code, experimental verification, literature research, and manuscript preparation. The author is responsible for the claims, evidence, and references.

References

1. Aikawa, Y., Nuida, K., Shirase, M.: Elliptic curve method using complex multiplication method. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences **E102.A**(1), 74–80 (2019). https://doi.org/10.1587/transfun.E102.A.74
2. Atkin, A.O.L., Morain, F.: Elliptic curves and primality proving. Mathematics of Computation **61**(203), 29–68 (1993). https://doi.org/10.1090/S0025-5718-1993-1199989-X, https://inria.hal.science/inria-00075302v1, preprint version dated 29 November 1991, INRIA RR-1256
3. Boudabra, M., Nitaj, A.: A new RSA variant based on elliptic curves. Cryptology ePrint Archive, Report 2023/1299 (2023), https://eprint.iacr.org/2023/1299, sections refer to Cryptography 7(3), 37 (2023), doi:10.3390/cryptography7030037
4. Broadhurst, D.: A 5061-digit semiprime (2005), https://web.archive.org/web/20190827000752/http://physics.open.ac.uk/~dbroadhu/cert/semgpch.gp, public certificate dated 12 March 2005

5. Bröker, R., Stevenhagen, P.: Constructing elliptic curves in almost polynomial time (2005), https://arxiv.org/abs/math/0511729v1, preprint
6. Cheng, Q.: A new class of unsafe primes. Cryptology ePrint Archive, Report 2002/109 (2002), https://eprint.iacr.org/2002/109
7. Cohen, H.: A Course in Computational Algebraic Number Theory, Graduate Texts in Mathematics, vol. 138. Springer (1993). https://doi.org/10.1007/978-3-662-02945-9
8. Cohn, H., Heninger, N.: Ideal forms of Coppersmith's theorem and Guruswami-Sudan list decoding. In: Chazelle, B. (ed.) ICS 2011. pp. 298–308. Tsinghua University Press (January 2011), https://arxiv.org/abs/1008.1284v2, full version (2013)
9. Cox, D.A.: Primes of the Form x^2+ny^2: Fermat, Class Field Theory, and Complex Multiplication. John Wiley & Sons (1989)
10. Demytko, N.: A new elliptic curve based analogue of RSA. In: Helleseth, T. (ed.) EUROCRYPT'93. LNCS, vol. 765, pp. 40–49. Springer, Berlin, Heidelberg (May 1994). https://doi.org/10.1007/3-540-48285-7_4
11. Dieulefait, L.V., Urroz, J.: Factorization and malleability of RSA moduli, and counting points on elliptic curves modulo N. Mathematics **8**(12), 2126 (2020). https://doi.org/10.3390/math8122126, https://arxiv.org/abs/1911.11004
12. Galbraith, S.D.: Elliptic curve Paillier schemes. Journal of Cryptology **15**(2), 129–138 (March 2002). https://doi.org/10.1007/s00145-001-0015-6
13. Galbraith, S.D., McKee, J.F.: Pairings on elliptic curves over finite commutative rings. In: Smart, N.P. (ed.) 10th IMA International Conference on Cryptography and Coding. LNCS, vol. 3796, pp. 392–409. Springer, Berlin, Heidelberg (December 2005). https://doi.org/10.1007/11586821_26, https://www.math.auckland.ac.nz/~sgal018/pair-mod-n.pdf, full author version
14. Goldwasser, S., Kilian, J.: Almost all primes can be quickly certified. In: 18th ACM STOC. pp. 316–329. ACM Press (May 1986). https://doi.org/10.1145/12130.12162
15. Hales, J.: Divisors in residue classes revisited. Journal of Number Theory **290**, 310–330 (2027). https://doi.org/10.1016/j.jnt.2026.03.014
16. Koyama, K., Maurer, U.M., Okamoto, T., Vanstone, S.A.: New public-key schemes based on elliptic curves over the ring Z_n. In: Feigenbaum, J. (ed.) CRYPTO'91. LNCS, vol. 576, pp. 252–266. Springer, Berlin, Heidelberg (August 1992). https://doi.org/10.1007/3-540-46766-1_20
17. Kunihiro, N., Koyama, K.: Equivalence of counting the number of points on elliptic curve over the ring Z_n and factoring n. In: Nyberg, K. (ed.) EUROCRYPT'98. LNCS, vol. 1403, pp. 47–58. Springer, Berlin, Heidelberg (May / June 1998). https://doi.org/10.1007/BFb0054116
18. Le Gluher, A., Spaenlehauer, P.J., Thomé, E.: Refined analysis of the asymptotic complexity of the number field sieve. Cryptology ePrint Archive, Report 2020/829 (2020), https://eprint.iacr.org/2020/829, journal version: Mathematical Cryptology 1(1), 1–18 (2021)
19. Lehman, R.S.: Factoring large integers. Mathematics of Computation **28**(126), 637–646 (1974). https://doi.org/10.1090/S0025-5718-1974-0340163-2
20. Lenstra, Jr., H.W.: Divisors in residue classes. Mathematics of Computation **42**(165), 331–340 (1984). https://doi.org/10.1090/S0025-5718-1984-0726007-1, https://pub.math.leidenuniv.nl/~lenstrahw/PUBLICATIONS/1984b/art.pdf

21. Martín, S., Morillo, P., Villar, J.L.: Computing the order of points on an elliptic curve modulo N is as difficult as factoring N. Applied Mathematics Letters **14**(3), 341–346 (2001). https://doi.org/10.1016/S0893-9659(00)00159-2
22. Nitaj, A., Fouotsa, E.: A new attack on RSA and Demytko's elliptic curve cryptosystem. Cryptology ePrint Archive, Report 2019/1050 (2019), https://nitaj.users.lmno.cnrs.fr/demytko2.pdf, full author version
23. Okamoto, T., Uchiyama, S.: Security of an identity-based cryptosystem and the related reductions. In: Nyberg, K. (ed.) EUROCRYPT'98. LNCS, vol. 1403, pp. 546–560. Springer, Berlin, Heidelberg (May / June 1998). https://doi.org/10.1007/BFb0054153
24. Reble, D.: Interesting semiprimes (2005), https://web.archive.org/web/20210216075050/http://www.graysage.com/djr/isp.txt, public semiprimality certificate dated 26 February 2005
25. Shirase, M.: Condition on composite numbers easily factored with elliptic curve method. Cryptology ePrint Archive, Report 2017/403 (2017), https://eprint.iacr.org/2017/403
26. Silverman, J.H.: Advanced Topics in the Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, vol. 151. Springer (1994). https://doi.org/10.1007/978-1-4612-0851-8
27. Silverman, J.H.: The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, vol. 106. Springer, 2 edn. (2009). https://doi.org/10.1007/978-0-387-09494-6
28. Sutherland, A.V.: Isogeny volcanoes. In: Proceedings of the Tenth Algorithmic Number Theory Symposium. The Open Book Series, vol. 1, pp. 507–530. Mathematical Sciences Publishers (2013). https://doi.org/10.2140/obs.2013.1.507, https://arxiv.org/abs/1208.5370
29. Vitto, G.: Factoring primes to factor moduli: Backdooring and distributed generation of semiprimes. Cryptology ePrint Archive, Paper 2021/1610 (2021), https://eprint.iacr.org/2021/1610, revision of 22 December 2021

A Alternative Reconstruction Arguments

Section 3 proves recovery by direct norm-lattice enumeration. We give an alternative through a prior small-root algorithm, then treat the ramified case excluded by the main theorem's coprimality hypothesis.

A.1 Reduction to Number-Field Small-Root Recovery

It suffices to treat two ordinary factors; the mixed and supersingular cases already have constant-size reconstructions in Section 3. We retain the notation $K = \mathbb{Q}(\sqrt{D})$, $\mathcal{O}_K = \mathbb{Z}[\omega]$, and $Z = \pi_p \pi_q$.

For a monic linear polynomial $f \in \mathcal{O}_K[X]$ and an integral ideal I, Cohn–Heninger [8, Theorem 1.3 of the full version] find all $w \in \mathcal{O}_K$ satisfying

$$|\sigma_1(w)| < B_1, \qquad |\sigma_2(w)| < B_2, \qquad \mathrm{Norm}\big(f(w)\mathcal{O}_K + I\big) > \mathrm{Norm}(I)^{\beta},$$

provided $0 < \beta \le 1$ and $B_1 B_2 < \mathrm{Norm}(I)^{\beta^2}$. Here σ_1, σ_2 are the two complex embeddings, and the ideal sum $f(w)\mathcal{O}_K + I$ is the ideal GCD appearing in their theorem. For fixed field degree, the algorithm runs in polynomial time in the explicit input length, including the supplied integral bases. In our quadratic setting, bases for $\mathcal{O}_K$ and $I = N\mathcal{O}_K$ are $(1, \omega)$ and $(N, N\omega)$, so the theorem applies with varying D.

Encoding the Frobenius Product. Equation (2) determines $Z \bmod S\mathcal{O}_K$ from (N, S, D). Choose a representative r by first centering its ω coefficient modulo S, then subtracting an integer multiple of S to center its real part. This gives

$$|\Re r| \le S/2, \qquad |\Im r| \le S\sqrt{|D|}/4.$$

The unknown correction $w = (Z - r)/S$ is an algebraic integer. Choose an integer v with $vS \equiv 1 \bmod N$ and set

$$I = N\mathcal{O}_K, \qquad f(X) = X + vr.$$

These inputs are computable from the public data. At the desired root,

$$Sf(w) = Z + (Sv - 1)r \in (Z).$$

Since $Z\overline{Z} = N$, we have $I \subseteq (Z)$, and $\gcd(S, N) = 1$ makes S invertible modulo (Z). Thus $f(w)\mathcal{O}_K + I \subseteq (Z)$ and

$$\mathrm{Norm}\big(f(w)\mathcal{O}_K + I\big) \ge N, \qquad \mathrm{Norm}(I) = N^2.$$

Verifying the Small-Root Bounds. Each $\pi_\ell = a + b\omega$ has $b \neq 0$, since otherwise its prime norm would be a square. Hence $\ell = |\pi_\ell|^2 \ge |D|/4$, giving $|D| \le 4\min(p, q) \le 4\sqrt{N}$. Using $|Z| = \sqrt{N}$ and $S > N^{1/3}$, we obtain

$$|w| \le \frac{\sqrt{N}}{S} + \sqrt{\frac{1}{4} + \frac{|D|}{16}} < N^{1/6} + \frac{1}{2}\sqrt{1 + \sqrt{N}} < \frac{4}{5}N^{1/4} \qquad (N \ge 2^{24}).$$

For the last inequality, division by $N^{1/4}$ bounds the preceding expression by $1/4 + \frac{1}{2}\sqrt{1+2^{-12}} < 4/5$. Both embeddings have the same absolute value, so take $B_1 = B_2 = (4/5)N^{1/4}$.

Put $L = \lceil \log_2 N \rceil$ and $\beta = 1/2 - 1/(4L)$. The ideal-GCD norm is then strictly greater than $\mathrm{Norm}(I)^\beta$, while

$$B_1 B_2 = \frac{16}{25} N^{1/2} < \frac{1}{\sqrt{2}} N^{1/2} \le N^{2\beta^2} = \mathrm{Norm}(I)^{\beta^2}.$$

The last inequality follows from $N \le 2^L$. Rational approximations to B_1, B_2 preserve these strict margins. The gap in the root-bound exponent is of order $1/\log N$, so the lattice parameters remain polynomial in the input length.

The small-root algorithm therefore lists w, from which $Z = r + Sw$ is recovered. Retain candidates of norm N satisfying the reconstruction congruences, then use the 25-sum search in Section 3 to obtain the factors. Trial division handles the finite range $N < 2^{24}$.

A.2 Ramification of the Common Prime

Retain the size and local-order hypotheses of Theorem 2, but suppose the odd prime S divides D and is coprime to N. Reduction of the norm form gives $\mathrm{Norm}(\pi - 1) \equiv (a + \nu b/2 - 1)^2 \bmod S$, so the first alternative forces $\ell \equiv 1 \bmod S$, while the second gives $\ell \equiv -1 \bmod S$.

These two possible residues determine either the sum or the difference of the factors up to two lifts. If both signs equal ϵ, then $p + q \equiv \epsilon(N+1) \bmod S^2$, with $0 < p + q < 2S^2$. If the signs differ, choose the ordering $p \equiv 1, q \equiv -1$; then $p - q \equiv 1 - N \bmod S^2$ and $|p - q| < S^2$. In either case, testing the two lifts with the corresponding integer square discriminant recovers the factors. The residues also permit recovery through Lenstra's rational residue-divisor algorithm, applied to ± 1, because $S^3 > N$.

B A Single-Lift Optimization

The Gaussian reconstruction in Section 5 tests 25 candidate Frobenius sums. The following public criterion certifies when its implementation may test only the centered representative.

Write $C = \pi_p + \pi_q$, $Z = \pi_p \pi_q$, and let σ be the Gaussian prime of norm S used there. Since $C \equiv Z + 1 \pmod{\sigma^2}$ and $|\sigma^2| = S$, the condition $\sqrt{p} + \sqrt{q} < S/2$ implies $|C/\sigma^2| < 1/2$. Both coordinates therefore lie in the central rounding cell, and nearest-coordinate reduction of $Z + 1$ modulo σ^2 returns C.

A sufficient condition can be checked with integer arithmetic. Put

$$L = S - 2\lceil \sqrt{S} \rceil + 1 \le (\sqrt{S} - 1)^2 \le \min(p, q).$$

For $L > 0$, define

$$H = \left(\lfloor \sqrt{L} \rfloor + 1\right) + \left(\left\lfloor \sqrt{\lceil N/L \rceil} \right\rfloor + 1\right).$$

Both factors lie in $[L, N/L]$. The function $\sqrt{x} + \sqrt{N/x}$ attains its maximum on this interval at an endpoint, so $\sqrt{p}+\sqrt{q} \le \sqrt{L}+\sqrt{N/L} \le H$. Thus $2H < S$ certifies the single-lift condition. Otherwise the algorithm retains the 25-candidate search proved in the main text; Appendix D.5 gives a case requiring a noncentral lift.

C Explicit CM Maps

The public-map method of Section 5 requires an evaluable endomorphism. We give the maps used for $D = -3, -7, -15$ in the experiments, their defining identities, and the conversion to the public curve models. Appendix D.6 gives worked scalar examples.

C.1 Discriminant -3

For $E_B : y^2 = x^3 + B$, with B a unit and residue characteristics greater than three, use

$$f(x) = -\frac{x^3 + 4B}{3x^2}, \qquad f'(x) = -\frac{x^3 - 8B}{3x^3}. \tag{8}$$

The rational identity

$$\frac{(x^3 + B)f'(x)^2}{-3} = f(x)^3 + B$$

verifies the curve equation for (7). The map fixes the identity, has degree three, and has differential $\sqrt{-3}$. It is consequently the trace-zero CM endomorphism with square $[-3]$. The maximal order is the Eisenstein order $\mathbb{Z}[(1 + \sqrt{-3})/2]$. This map presents its trace-zero element in the form used in Section 5.

For $D = -4$, the Gaussian algorithm uses the automorphism i. Composing it with doubling gives the trace-zero endomorphism $2i$ with differential $\sqrt{-4}$, fitting the present formulation.

C.2 Discriminant -7

Start with

$$E_0 : y^2 = x^3 - 35x - 98, \qquad j(E_0) = -3375.$$

Its CM order is $\mathcal{O}_{\mathbb{Q}(\sqrt{-7})}$, with class polynomial $H_{-7}(T) = T + 3375$. Put

$$\begin{aligned} k(x) &= x^3 + 7x^2 - 21x - 91, \\ n(x) &= -x^7 - 14x^6 - 343x^5 + 588x^4 \\ &\quad + 24353x^3 + 120050x^2 + 285719x + 422576, \\ f_0(x) &= \frac{n(x)}{7k(x)^2}. \end{aligned}$$

The polynomial k is the kernel polynomial of a degree-seven isogeny. Composing that isogeny with an isomorphism of its codomain with E_0 over $\mathbb{Q}(\sqrt{-7})$ gives the map above. The defining identity

$$\frac{(x^3 - 35x - 98)f_0'(x)^2}{-7} = f_0(x)^3 - 35f_0(x) - 98 \tag{9}$$

verifies the curve equation. The resulting map fixes the identity, has degree seven, and has differential $\sqrt{-7}$. In characteristic zero the differential map on endomorphisms is injective [26, Chapter II, Proposition 1.1 and Theorem 2.2], so $\psi^2 = [-7]$; the identity specializes to good reductions away from the excluded characteristics.

For a quadratic twist $E_c : y^2 = x^3 - 35c^2x - 98c^3$, use

$$f_c(x) = cf_0(x/c), \qquad f_c'(x) = f_0'(x/c).$$

The twist parameter can be recovered from the public short Weierstrass coefficients as $c = 5B/(14A)$ when the denominator is invertible. Substitution gives $A = -35c^2$, $B = -98c^3$, so this conversion applies to every regular public model of this invariant.

C.3 Discriminant -15

Here the Hilbert class polynomial and a chosen root are

$$H_{-15}(T) = T^2 + 191025T - 121287375, \qquad j = \frac{-191025 + 85995\sqrt{5}}{2}.$$

Work over $F = \mathbb{Q}(\sqrt{5}) = \mathbb{Q}(j)$ on $E_0 : y^2 = x^3 - 3kx + 2k$, $k = j/(j - 1728)$. Construct the degree-three isogenies whose codomain has the conjugate invariant, then the degree-five isogenies returning to invariant j. Among their composites, select an isomorphism of the final codomain with E_0 over $F(\sqrt{-15})$ whose composite differential squares to -15. Such a composite exists because the norm-three and norm-five ideals multiply to the principal ideal generated by $\sqrt{-15}$. An automorphism fixing F sends the differential to its positive or negative, hence sends the endomorphism to ψ or $-\psi$. The two signs have the same x-map, so that map is defined over F. The resulting $f_0 \in F(x)$ has numerator degree 15 and denominator degree 14. It satisfies the exact identity

$$\frac{(x^3 - 3kx + 2k)f_0'(x)^2}{-15} = f_0(x)^3 - 3kf_0(x) + 2k,$$

which was verified symbolically. This example uses class number two.

For a scalar public invariant modulo N, evaluate the coefficients using

$$\sqrt{5} = \frac{2j + 191025}{85995} \pmod{N},$$

and convert to the public model using $c = -3B/(2A)$ and $f_c(x) = cf_0(x/c)$. All displayed denominators must be units; a proper denominator GCD reveals a factor.

D Factorizations and Test Instances

This appendix supplies the numerical evidence for Section 8: the recovered factors of the published certificates, worked recovery examples, and cases exercising the composite-order algorithm. Concatenate the lines within each digit block to obtain the integer. Section 8 gives the timings and validation procedure.

D.1 Broadhurst's 5061-Digit Modulus

The input is Broadhurst's public certificate of 12 March 2005 [4]. The public-point method recovers the factors below from (N, S, A, X, Y); norm reconstruction recovers the same pair from (N, S). Their product is the published modulus.

p (2531 Digits)

```
22163854734148895812170045804151188464746184595616104428548990
16487305568615914137770515551287703154919538283393858460669504
34874472878062813089231694841090833918918758150300396742906806
69951598144519972858971906762134057950536281802253719148308017
30373489372078451902276007852882230395119208657232358705092649
06291806898160198080635927668791006429146140965141470974714479
95841473555787651348461843017160397342445092447862752386563647
88038978886337582870689506672480144274747834926579675683885600
77659269180589351128366086935008694852293862525189397341189809
08078882449139052213623727634578127549909268623014501898072390
70538502730882862719222188234092631522960852387963834784985240
41597615683058322342186029056887146617981868888182118516785978
22761139810302724211844553104992650406653310700972223523848500
53536066639099724483559309268738039568253365402547822490414747
81505403571212109480974578616079559863537133494748672591425530
38428647987535034538980951699486873688074372561562693042262823
05019517432111744078040722674893279581513334252551052868986933
70756206917074501876432637872376039056930304907586846764595945
88157777580201755923658867434007953418603093907178763661484839
38194297715964455708390878829881974598907388569320846689549338
13791109229180814867651269419075380557909299228671342576779998
55149038099621160789750367003401961783341312412681496592243582
13262251974059302815619763107548803144521678104437940996888612
82927071176464546877290295460222205227024698478121481770949855
65448085681476359522036351234238644930595094150852128875488310
87898087925380893471421986151776902601447794834936428787155205
39437254194663227442949455492508635500865172508543192999712904
70247577476815635016798151363910073414416907999644684113000050
36699904253260999893317980935085928709281607993314779165486647
00041094350669863550122957700843579316219734687444950500933079
64919476635237755903877907308975330318599940237292772131375606
```

730425835999268879120863994671221692890199990521128596000117004476488600385411646312414147980809344494717531825847204968784821494481394575496280480953672192968654723282236651698782925752217069218583709937891178793458627323606067037791284312838557544275726527362811200179949360726290107450449110958609211693911530194588717892856537331093364668059063968153288560922755366345257283646733991157614279808850040389059553240804342060496143111798488620773010839523795728968855049129069316944890497817588406328461559941779438717841179415090903205435093161840457120166479082298828583058382448466715023822702149059283057

q (2530 Digits)

814427249997044536351984084647697207137866791536129977449924813816162555668707237286396466402346708029875494152034266035784743044060976812611583207284099907189233835003043600742034941775650255758285843078496095411158388015133664697072204034897265313800182804838487407874426150199097666803720390445108165042619722572530154358321720587868496720474500279814968435171216012356875854379835091190315588749826894009726099067246836711812561404527722483595525784927499178192136974798427927487237760532255177899064671800286250387590800323010527433511783755719540734573424871879101450802394050776860919253961027904152489284442899217093718367024301155451455793523008795792417647262954373245070268504371972655516048987276665791922309207674824337378314318898397203964610897338752537384867978934644949557186747899565650089669666979923127892164887919596623878224344611177712702822434848498926428438874587657442909025340866323497509234488125094290895123707394374313432593887695927462505991302998797294336667760001844887229685233057032978853162899967513333449055949631726839392073293325614209010011822017056344082415047888214491159246961537701300202773414754593968859171832313637037548814555590857928639879174260037949725350693568129065346435461272480899387947413507187120466011732790247317708756951260291396467453061802193170479763868071182384877258840798995166413525637213429223375618001783947223625273299679242936475474110988084395113094018420690814634170296588174186742454884408942362572111402968066009413590204023045183070713856976193197235647197168246608247154043911568808716764687620528372825884895014611700772811948659589417316967019410343087650839126490210032245882877251884229502624134469059999053623489807841159374195256526775696234805958408710982731786672777822569032184677914935341513682015986600927808989838196739647392157994651611458261871885250055076742973636144574543963366180977051993843206937275937827081209065658535931443468190267940616151036358526517628689995115373029960062920898338476168041132037050376682753511327683273788515966668726122 4

93261063527420224717930971021392427632890245833801215485584220
82940578599276408600469642275348286832036327068323595659453861
93475632658638145294275566517076525245976520048149993009441438
88338397782592905265902620600509448449099808236888101473367 82
07511174184427909542228615932582306963990043436860946270899821
05057135837538575039507080790900580884413952135483060196032653
05248492380155159507308753992430466820005366318068682301898665
96347961485111260084882740653876373348648466523993

D.2 Broadhurst's Curve Orders

The recovered Frobenius elements determine the local orders through

$$\mathrm{Norm}(\pi_\ell - 1) = \ell + 1 - 2\Re(\pi_\ell).$$

For this instance the exact checks $S^2 > 16p, 16q$ show that each Hasse interval contains at most one multiple of S. Thus the full order is obtained by rounding $(\ell+1)/S$ to the nearest integer and multiplying by S. The results are $4Sr_p$ and $4Sr_q$, where both r_p, r_q have 840 digits. Both r_p, r_q pass probable-prime tests and have not been independently certified prime.

D.3 Reble's 1084-Digit Modulus

Reble's certificate [24] supplies N, A, s, t and an affine point. Here s, t denote his Q, T, respectively. The quadratic-twist method of Section 4 recovers the following factors from (N, A, s, t).

p (543 Digits)

11720990044176604485656482285369732810060846386219272085536405
87253760948011511585395454559143032247641663618272332076279747
48555580785918469406861654147386441510559363392715817728672245
69938522208974709445440698121693586713136011742194739741899723
13862484260214327281073952472107837948499063449221486753727501
53154323991759587128290262415063090969439615092699624981254513
80111721708681418118874268076687305476680921066115071942491901
61039457888471652840283101415828578539308440266178942657944304
70237075098737394801950735228563440292113831261

q (542 Digits)

20083837878225401365247454652399288511943664897737051292330162
04538079847047967553624738053694816692363354958717219555398238
27845656971407635199873386941295582613528886860458159891305742
27981277228050495962920464112804540856578175224873773598186424
15050009192403216957026792723167602746296336758526213630623424
95323688040923768261759594342438464082084477170767532502558171

```
14025968035788584965691819688050824429127525800543566346284978
92919177981124109486546697620160365041422004274633872543643826
80603491377968436127402932630579659919810901 81
```

The successful trial uses twist parameter $c = 7$, input $x = 3$, and scalar $k = 4st$. The GCD of the resulting projective denominator with N gives a proper factor.

D.4 A CM Generation Example

The 142-bit Gaussian certificate constructed by the method of Section 2.1 has public values

$$\begin{aligned} N &= 461213270445327308908609968651695598292733, \\ S &= 538606233865081, \\ A &= 209211474491737248721536592953732992453690 3, \\ X &= 357928980691994121443225647287286193142971 1, \\ Y &= 141544371226266299492634976062517106866485 3. \end{aligned}$$

The recovered factorization is

$$N = 556886529430039208669 \cdot 8281997248476609399457.$$

D.5 Prime-Order Examples

The following factor-and-order combinations test the branches of Theorem 3.

p	q	S	Branch
1933	1993	1009	Gaussian reconstruction
1933	275837	1009	Noncentral Gaussian lift
1933	12107	1009	Mixed reduction
12107	56503	1009	Supersingular, $S \equiv 1 \pmod 4$
12227	36683	1019	Supersingular, $S \equiv 3 \pmod 4$

The second case uses the public curve $y^2 = x^3 + 507540083x$ modulo $N = 533192921$ and point $P = (243953086, 34787680)$. Taking $\lambda = 469$ gives $\sigma = 28 + 15i$ and $C = -356 - 408i$, whereas the central remainder is $203 + 432i$. Here $C = C_0 - \sigma^2$, demonstrating the need to check noncentral lifts.

D.6 Public-Map Examples

The following examples give full certificates and their recovered Frobenius elements. For each, recovery uses (N, S, A, B, X, Y) and the corresponding map in Appendix C. Trial division verifies the small primes, and enumeration of all affine points and the identity verifies the local curve orders.

Discriminant -3. Take

$$N = 78626761, \qquad S = 739, \qquad E : y^2 = x^3 + 1,$$
$$P = (48823350, 15863679).$$

The point is on the curve, $[739]P = \mathcal{O}$, and the size threshold holds. Choosing $\lambda = 641$ gives $\lambda^2 = -3 \pmod{739}$. The root formula of Section 5 yields $r = 300308$ with $r^2 = -3 \pmod{N}$. Writing $\omega = (1 + \sqrt{-3})/2$, reconstruction gives

$$Z = -4451 - 5760\omega, \qquad C = 2, \qquad \pi_1 = 75 + 32\omega, \quad \pi_2 = -73 - 32\omega.$$

Their norms are 9049 and 8689, respectively, so

$$78626761 = 8689 \cdot 9049.$$

Both curve orders are $8868 = 12 \cdot 739$, in agreement with $\mathrm{Norm}(\pi_1 - 1) = \mathrm{Norm}(\pi_2 - 1) = 8868$.

Discriminant -7. Take

$$N = 335707, \qquad S = 107, \qquad E : y^2 = x^3 - 35x - 98,$$
$$P = (324939, 51564).$$

Here $[107]P = \mathcal{O}$, the size threshold holds, and $\lambda = 10$ is a square root of $-7 \pmod{107}$. The degree-seven map yields $r = 99010$ with $r^2 = -7 \pmod{N}$. For $\omega = (1 + \sqrt{-7})/2$, reconstruction gives

$$Z = -139 + 434\omega, \qquad C = -6 - 18\omega, \qquad \pi_1 = 15 - 22\omega, \quad \pi_2 = -21 + 4\omega.$$

The corresponding norms are 863 and 389, giving

$$335707 = 389 \cdot 863.$$

The exact orders are $\#E(\mathbb{F}_{389}) = 428 = 4 \cdot 107$ and $\#E(\mathbb{F}_{863}) = 856 = 8 \cdot 107$, matching the Frobenius traces.

Larger Instances. For $D = -3$, public-point reconstruction factored a 1019-bit modulus on $y^2 = x^3 + 7$ in about 0.013 seconds. For $D = -7$ it factored a 1017-bit modulus on the twist $c = 5$ in about 0.013 seconds. For $D = -15$ it factored a 1022-bit modulus, again with twist $c = 5$, in about 0.014 seconds. The timing procedure is that of Section 8. For these larger examples, the factors and S passed probable-prime tests; separate primality certificates were not generated.

D.7 A Nonprincipal Torsion Ideal

A separate experiment tests ideal reconstruction for $D = -23$, where the class number is three. With

$$S = 785640672212380837,$$

the selected ideal $\mathcal{S}$ has norm S but smallest nonzero element norm $2S = 1571281344424761674$. Thus it is nonprincipal. Nevertheless, the same lattice reconstruction, supplied with the oriented roots r and λ, returns

$$124313655666817997182724779725717786194060911$$
$$= 7617571957596998260223 \cdot 16319328042952070893457.$$

Here the input includes r, λ, constructed from the known factors, so the experiment isolates the ideal-reconstruction stage.

D.8 Composite-Order Examples

The following eleven cases test the algorithm of Theorem 4, with recovery input (N, A, P) and the certified factorization of M. The local primes and order factorizations were independently certified, and the curve equations, exact point orders, and size thresholds were checked.

p	q	M	Case
2269	2153	1105	Split eigenlines
10861	44381	1105	Both 5-eigenspaces
8010901	32044301	160225	Both 25-eigenspaces
55621	55541	5525	Unequal 5-adic exponents
20113	19717	3315	Inert prime three
17417	17713	4420	Annihilator exponent three
17417	17713	4420	Annihilator exponent four
55621	55541	5525	Local annihilators differ
179	16381	180	No eigenline, mixed reduction
8191	20479	1024	Supersingular, power of two
472391	1180979	59049	Supersingular, power of three

In the mixed example, $M = 180 = 2^2 \cdot 3^2 \cdot 5$, the local curve orders are 180 and 16200. The order-five projection is not an eigenvector at the ordinary factor. The root-extraction tests therefore fail, but the small-cofactor search gives $\gcd(M - 1, N) = 179$.

E Private Isogeny Descent: Construction and Limitations

Section 6 describes the construction and the known-field recovery attack. Here we give the sampling lattice, the path-selection rules, and the public parameters of the 1024-bit example, then discuss constructions with distinct local fields.

E.1 Generating the Local Curves

Choose $S \equiv 1 \pmod 4$, a Gaussian integer $\sigma = a + bi$ of prime norm S, and $f = 2^k$ with $k \geq 1$. Multiply σ by a unit so that a is odd. The condition $f \mid \mathrm{Im}(\sigma\alpha)$ for $\alpha = u + vi$ defines

$$L_f = \{(u, v) \in \mathbb{Z}^2 : bu + av \equiv 0 \bmod f\}.$$

Since a is invertible modulo f, a basis is $(1, -ba^{-1} \bmod f), (0, f)$, of determinant f. Reduce this basis before sampling bounded coefficients. This enforces the congruence directly, even when f exceeds the target coordinate bounds.

For $\pi = 1 + \sigma\alpha$, retain candidates with odd real part, $v_2(\operatorname{Im}\pi) = k$, and prime norm $p > 3$. Here v_2 is the exact exponent of two in a nonzero integer. Prime-search running time is heuristic; the recorded instance has proved prime factors. A quartic twist of a Gaussian curve realizes the order

$$\operatorname{Norm}(\pi - 1) = S \operatorname{Norm}(\alpha).$$

Multiply random points by the private cofactor $\operatorname{Norm}(\alpha)$, retaining a nonzero point whose order is verified to be S.

The 2-part of $[\mathbb{Z}[i] : \mathbb{Z}[\pi]]$ is 2^k, so the rational 2-isogeny volcano has depth k. At the initial $j = 1728$ curve, choose a descending edge with different codomain invariant. At each subsequent level, exclude the edge just traversed and choose another rational 2-isogeny. The repeated edges caused by the initial automorphisms have the same codomain and conductor index. The volcano structure, including the case $j = 1728$, is described in [28].

The composite $\phi : E_0 \to E_k$ has degree 2^k, so it preserves the transported point's odd order S. At the floor,

$$\operatorname{End}(E_k) = \mathbb{Z} + 2^k\mathbb{Z}[i], \qquad \Delta_k = -4 \cdot 2^{2k}, \qquad h(\Delta_k) = 2^{k-1},$$

and the unique rational 2-isogeny ascends. These facts provide local checks on the path. Repeat at q and combine the endpoint coefficients and points by CRT as in Section 6.

E.2 Endomorphism Degree After Descent

For integers c, d with $d \neq 0$, each endpoint endomorphism $c + fdi$ has degree $c^2 + f^2d^2 \geq f^2$. The trace-zero element fi attains this minimum; the literal $\sqrt{\Delta_k} = 2fi$ has degree $4f^2$. The private composite $\phi \circ i \circ \widehat{\phi}$ evaluates fi under the compatible identification of endomorphism algebras. Its expression uses the retained path. The known-field attack instead uses the public N, S and unchanged fundamental discriminant -4, as proved in Section 6.

E.3 Parameters of the 1024-Bit Example

The certificate reported in Section 8 uses $k = 110$. Its endpoint order discriminant is -2^{222}, its minimum noninteger endomorphism degree is 2^{220}, and $S/(N^{1/6} + 1)^2 \approx 433.4$. The public curve is $y^2 = x^3 + Ax + B$ with point $P = (X, Y)$ and the following parameters. Concatenate wrapped digits within each entry.

```
N =
148181865176918517320889636159835116772887173581333537460367
119209626153659380604150872207140591098254516471524708398267
```

```
819950431801853376656938712236024042974876014095285646333166
297223105825206229084476531249141567321411312490984461636313
596608018944939404750132284479758856006722390909191055310220
440581321

S =
229349861599007151161082089530208694079656498916828112373758
883938692287608848480807001855311012568655511 3

A =
214150621499876705880651193007897822017270944692076220572013
755694846169409307962326310542326684695404802896218182993203
490081933130834107904615399365290805670622019473874876319050
935797501454359491063991409194726435073292797047640284128837
336323725033350047260213243718767083891042903663260014356860
57128534

B =
745870732521574872643046078917485365361331670785948484453763
759637400346538556139835981312819293911653503868389918750065
692799122830222242828682415461063638780513938296195194659140
007404107640474135116214853758340660295099575163926722575705
411190901317334851278289710998001461154635580336169813556914
66453687

X =
822048421119202887216971235287459617022348409584525676187641
424280260822131745755685407255472340920807014361967238974347
990463334152413006640516103474673638133786139285617120071801
062660598549679425332135300684762976443101576964292843066264
375866311878162780952862542200753162534149388563420308482408
09577259

Y =
186029181383436616702114507521930387037035650454407620915701
269533336765769812027974508031408450690372559412307558282946
111830371920463708638747190827222247265502172983598885253362
126018126803328095383416948215996167080125557400436336663496
834999401837412715468789543626724341151529522600567422492061
41852641
```

The local orders were independently counted, S, p, q were proved prime, and good reduction and $[S]P = \mathcal{O}$ were checked. The certificate threshold also has an exact integer check. Put

$$A_S = S^3 + 15S^2 + 15S + 1 - N, \qquad B_S = 6S^2 + 20S + 6.$$

Expanding $(\sqrt{S}-1)^6$ shows that $N < (\sqrt{S}-1)^6$ is equivalent to $A_S > 0$ and $A_S^2 > B_S^2 S$.

For each discriminant

$$-3, -4, -7, -8, -11, -15, -16, -19,$$
$$-20, -23, -27, -28, -43, -67, -163,$$

the class-polynomial GCD at the endpoint invariant equals one. These are the specific small-order fingerprints tested.

E.4 Distinct Fields and Endpoint Polynomials

For an ordinary trace t_ℓ at characteristic ℓ, write

$$n_\ell = \ell + 1 - t_\ell, \qquad t_\ell^2 - 4\ell = Dv^2.$$

The endomorphism conductor divides v, so rational 2-descent from a maximal order has depth at most $v_2(v)$ [28, Sections 2.11–2.12]. Descent preserves n_ℓ. A construction at fixed primes must therefore arrange the common divisor before descending.

The distinct-field tests in Section 8 use $D = -4, -8$. At depth six the endpoint discriminants are -16384 and -32768, whose class polynomials have degrees 32 and 64. Their evaluations distinguish the two factors, enabling the class-polynomial GCD test of Section 6. This explains the recovery despite the failure of the starting-field norm tests and the small-discriminant tests above.

For a Gaussian endpoint of depth $k \geq 1$, the class-number formula gives degree 2^{k-1}. Thus the tested depth-twelve polynomial has degree 2048, while the deepest endpoints at depths 83, 166, and 333 have degrees 2^{82}, 2^{165}, and 2^{332}. Section 8 reports the measured attacks; the deepest polynomials were not computed. These degrees measure the size of the dense polynomial representations; the best factoring attack on the deeper cases remains open.