Provable Recovery of RSA Private Exponents below $N^{11/42-\varepsilon}$

Yiming Gao[1] Honggang Hu[1,2]

[1]School of Cyber Science and Technology, University of Science and Technology of China
qw1234567@mail.ustc.edu.cn

[2]Hefei National Laboratory, Hefei, China
hghu2005@ustc.edu.cn

Abstract

Wiener's continued-fraction attack gives the classical provable bound $d < N^{1/4}$ for balanced RSA. Boneh and Durfee reached the exponent $1 - \sqrt{2}/2 \approx 0.2929$, but their argument relies on a heuristic independence assumption. We prove the first fully provable improvement beyond Wiener's $1/4$ exponent: for every fixed $\varepsilon > 0$, balanced RSA with $e = \Theta(N)$ can be factored deterministically in polynomial time whenever $d \leq N^{11/42-\varepsilon}$.

1 Introduction

Let $N = pq$ be an RSA modulus and let e be the public exponent. The private exponent is the least positive integer d satisfying

$$ed \equiv 1 \pmod{\varphi(N)}.$$

The problem of recovering RSA keys with a small private exponent asks for which ranges of d the factorization of N, and hence the private key, can be recovered efficiently from the public pair (N, e). We study the standard balanced setting $p < q < 2p$.

Wiener's continued-fraction method establishes the classical provable exponent $1/4$ for this problem [Wie90]. Coppersmith's original results give rigorous algorithms for finding small roots of univariate modular equations and bivariate integer equations [Cop96b, Cop96a]. Boneh and Durfee extend the lattice approach to multivariate modular equations and reach the larger exponent $1 - \sqrt{2}/2$, with a heuristic assumption in the root extraction step [BD99, BD00]. Herrmann and May later gave a linearized version of this construction [HM10].

In these multivariate lattice attacks, a determinant bound certifies that a sufficiently short polynomial vanishes at the hidden RSA root. This is only a vanishing certificate: it does not by itself show what information the certified equations provide about the root or whether they support an effective recovery procedure. A separate root-recovery argument is therefore needed. Boneh and Durfee express this missing guarantee by assuming that "the two shortest vectors in an LLL reduced basis give rise to algebraically independent polynomials" [BD99, BD00]. Proving the required independence has remained an open problem [MNV21]; related root-extraction questions also arise in more general multivariate modular Coppersmith constructions [Rya25].

Bauer and Joux [BJ07] addressed this issue in the trivariate integer setting by treating the known relations as an ideal $I = (p_1, p_2)$. They use a truncated Gröbner basis to describe the part of I supported on a prescribed monomial set, and an orthogonality-based lattice construction then yields a short polynomial $p_3 \notin I$. Their result, however, requires additional structural conditions on the ideal and the monomial set, so general RSA small-exponent attacks still rely on a heuristic independence claim.

Our proof takes a different route. We factor the first exact relation and treat each component that may contain the RSA root separately. Components that determine a secret value are solved

directly. For each remaining irreducible factor H that vanishes at the RSA root, quotient lattices or an integral-jet construction produce a second polynomial G that vanishes at the RSA root and is coprime to H. In the two-variable representation, resultant elimination then yields a finite set of candidates containing the RSA root. These candidates are checked against the RSA equations.

This gives the following provable improvement over Wiener's bound.

Theorem 1.1 (Balanced RSA 11/42 bound)**.** *Fix $\varepsilon > 0$. Let $N = pq$, where p, q are primes with $p < q < 2p$, and let the public exponent satisfy*

$$1 < e < \varphi(N), \qquad \gcd(e, \varphi(N)) = 1, \qquad e = \Theta(N).$$

Let d be the least positive integer satisfying $ed \equiv 1 \pmod{\varphi(N)}$. If

$$d \leq N^{11/42-\varepsilon},$$

then a deterministic algorithm factors N from (N, e) in time polynomial in $\log N$.

The exponent $11/42 \approx 0.2619$ is larger than $1/4$, so the theorem improves Wiener's rigorous range.

method	exponent for d	root extraction status
Wiener	$1/4$	rigorous
Boneh–Durfee	$1 - \sqrt{2}/2$	heuristic
this work	$11/42$	rigorous

Organization. Section 2 outlines the proof and explains the role of each construction. Section 3 introduces the scaled coefficient norm, graph ring, quotient lattices, and elimination tools used later. Section 4 constructs the rank-eight front lattice and derives the exponent $11/42$. Sections 5 and 6 turn the first relation into a finite list of components and construct the level lattices needed to handle them. Section 7 treats the linear and quadratic components, while Section 8 handles the two cubic regimes. Section 9 assembles the branches and performs the final exact verification.

2 Overview of Our Techniques

The proof separates the construction of an exact relation from the recovery of its root. A rank-eight lattice supplies the first relation P_3 and determines the exponent $11/42$. Its special form reduces root extraction to components of degree at most three in suitable coordinates. Quotient lattices handle the linear and quadratic components. For a cubic component, we use either a direct quotient or integral Taylor conditions, depending on the size of its coefficients. This section explains how these constructions fit together.

Throughout, $\log_e$ denotes the logarithm with base the RSA public exponent e and log and ln denote natural logarithms.

2.1 The Herrmann–May linearization and root bounds

We use three coordinates: the quotient in the RSA congruence, the factor sum, and an auxiliary coordinate that makes the RSA expression linear. Define x_0 by

$$ed - x_0\varphi(N) = 1,$$

and set

$$A = N + 1, \qquad y_0 = -(p + q), \qquad u_0 = 1 + x_0 y_0.$$

The coordinate y_0 records the factor sum, while u_0 absorbs the product x_0y_0. Since $\varphi(N) = N + 1 - (p + q) = A + y_0$, we obtain

$$ed = 1 + x_0(A + y_0) = Ax_0 + u_0. \tag{1}$$

Moreover,

$$1 \le x_0 < d, \qquad \gcd(x_0, d) = 1. \tag{2}$$

Since $e < \varphi(N)$, we have $x_0 = (ed - 1)/\varphi(N) < d$, and any common divisor of x_0 and d would divide $ed - x_0\varphi(N) = 1$.

Following Herrmann–May, introduce an independent variable u subject to the relation

$$xy - u + 1 = 0, \qquad \bar{f}(x, u) = Ax + u. \tag{3}$$

The graph relation makes $Ax + u$ equal to $1 + x(A + y)$. At the target, $\bar{f}(x_0, u_0) = ed$, so its m-th power is divisible by e^m. This divisibility is the input to the later Howgrave–Graham argument.

The lattice uses public bounds for the three root coordinates. For each dyadic range for d, let X be its upper endpoint and set

$$Y = 3\lceil\sqrt{N}\rceil, \qquad U = XY.$$

On the range containing d, we have $x_0 < d \le X$. The balance condition gives $p + q < 3\sqrt{N}$, so Y bounds the factor sum. The graph relation then gives $|u_0| = |1 + x_0y_0| \le XY = U$. These are the scales used in the scaled coefficient norm.

Proposition 2.1 (RSA root coordinates)**.** *For every upper endpoint X of a dyadic range satisfying $d \le X$, the integers (x_0, u_0, y_0, d) satisfy*

$$x_0y_0 - u_0 + 1 = 0, \qquad \bar{f}(x_0, u_0) = Ax_0 + u_0 = ed,$$

and

$$1 \le x_0 < d \le X, \qquad \gcd(x_0, d) = 1, \qquad |y_0| \le Y, \qquad |u_0| \le U.$$

The algorithm tries $O(\log N)$ ranges for d. One of them has an upper endpoint X satisfying $d \le X < 2d$. Proposition 2.1 records the bounds available on that range. These bounds scale every coefficient lattice below.

Recovering $y_0 = -(p + q)$ immediately factors N. Alternatively, a verified pair (x_0, d) determines $\varphi(N) = (ed - 1)/x_0$, and hence also determines the factors.

2.2 The front rank-eight lattice

The first lattice produces an exact polynomial relation at the hidden root. It follows the linearized construction of Herrmann and May [HM10]. After reducing by the graph equation $xy - u + 1 = 0$, it uses the eight level-three shifts

$$\mathcal{S}_3 = \{e^3x^2,\ e^2x\bar{f},\ e\bar{f}^2,\ e^3x^3,\ e^2x^2\bar{f},\ ex\bar{f}^2, \bar{f}^3,\ \mathrm{NF}(y\bar{f}^3)\}.$$

Here NF denotes graph normal form. Each shift evaluates to a multiple of e^3 at the hidden root, so the same is true for every integer combination. Their scaled coefficient vectors form a rank-eight lattice L_3 whose triangular matrix has determinant

$$\det L_3 = e^{12}X^9YU^{12}.$$

Write $X = e^\delta$. Since $e = \Theta(N)$, we have $\log_e Y = 1/2 + o(1)$, and $U = XY$. Therefore

$$\log_e \det L_3 = \frac{37}{2} + 21\delta + o(1).$$

Since the rank is 8, a shortest nonzero vector has length bounded by a constant times $(\det L_3)^{1/8}$. The Howgrave–Graham bound requires this length to be smaller than a fixed constant times e^3. At the exponent level, the required inequality is

$$\frac{37}{2} + 21\delta < 24 \quad \Longleftrightarrow \quad \delta < \frac{11}{42}.$$

Below this threshold by any fixed margin, solving the shortest vector problem (SVP) exactly and applying the Howgrave–Graham lemma produces an integer polynomial P_3 satisfying

$$P_3(x_0, u_0, y_0) = 0.$$

All lattice dimensions used here are fixed independently of N, so exact SVP runs in polynomial time in the input bit length. Shortestness also constrains the form of P_3, as used in Section 5. The determinant calculation yields $11/42$, but P_3 is only one equation in several coordinates. Root extraction therefore begins by factoring P_3 and analyzing its components.

2.3 Factorization of the first relation

The eight shifts give the relation a special form. Put $t = \bar{f}$. Since $t(x_0, u_0) = ed \neq 0$, we can invert t and introduce the ratio

$$z = \frac{ex}{t}.$$

At the RSA point, $z_0 = x_0/d$. In these coordinates, a pair of one-variable polynomials represents the first relation:

$$\frac{P_3}{t^3} = C(z)y + D(z).$$

A common factor $\chi(z) = \gcd(C, D)$ is already useful: if it vanishes at the target, the reduced numerator and denominator of its rational root $z_0 = x_0/d$ recover (x_0, d). Otherwise, dividing C, D by χ gives a coprime pair (C', D') defining the component containing the target, $C'(z)y + D'(z) = 0$. Its *canonical degree* is $\max\{\deg C', \deg D'\}$, which is at most three. An integral change of coefficients turns this component back into a factor H_r in the original graph coordinates.

The components that may contain the target therefore fall into three cases:

(i) an equation involving only z, whose rational root $z_0 = x_0/d$ recovers the coprime pair (x_0, d);

(ii) a canonical degree-zero equation, which fixes y_0 and therefore recovers $p + q$;

(iii) an irreducible factor H_r of canonical degree $r \in \{1, 2, 3\}$.

The first two cases give direct recovery. The factors H_1, H_2, H_3 are the remaining root extraction cases, and each will be supplied with a second relation.

2.4 Quotient lattices and a second relation

Once a component H is known, its multiples vanish everywhere on that component and give no further information about the target. We therefore identify all multiples of H in a suitable level lattice and project orthogonally away from their span. This constructs the quotient by the saturated sublattice of known multiples. Every nonzero quotient vector is represented by a rational polynomial outside the principal ideal (H).

The key point is that projection preserves evaluation at the target: it subtracts only a multiple of H, and H vanishes there. Although the projected coefficients may be rational, the value still equals that of an integer level-m lattice vector and is therefore in $e^m\mathbb{Z}$. If the projected vector is sufficiently short, the Howgrave–Graham argument forces this value to be zero. Clearing denominators gives the required second exact relation.

The determinant estimates for the linear and quadratic components apply for $\delta < 1/3$ and $\delta < 9/34$, respectively. Both thresholds exceed $11/42$, so these components can be handled throughout the target range.

2.5 The cubic branch: direct quotients and integral jets

For a cubic component, the method depends on the height of H_3, which measures its scaled coefficient norm. A large height increases the covolume of the lattice of known multiples. Dividing the ambient lattice determinant by this covolume gives a smaller quotient determinant and hence a sufficiently short second relation. Thus the direct quotient argument handles all factors above a suitable height threshold.

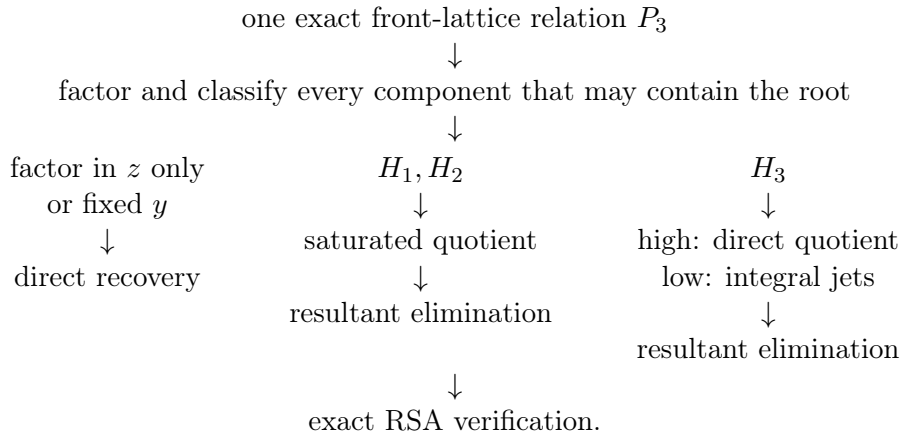
For the remaining factors, we use the rational parametrization of the cubic curve. Substituting it into a lattice polynomial and clearing denominators gives an integral binary form. We then require several initial Taylor coefficients of this form to vanish in a chosen projective coordinate chart; these are the integral-jet conditions. They define a sublattice of the quotient in which we seek a short nonzero vector. A small height bounds the coefficients of the parametrization and, in turn, the determinant cost of these extra conditions.

The Taylor conditions give an integer identity at the RSA root. The lattice bound makes the resulting integer small, while coprimality gives a lower bound if it is nonzero. To make these bounds incompatible, we choose a chart where the relevant common divisor is small. A resultant argument shows that one of $O(\log e)$ charts has a common divisor bounded by a fixed power of $\log e$. The integer must then vanish, giving a second exact relation outside (H_3). The direct quotient and integral-jet estimates together cover every cubic factor; Section 8 gives the thresholds and the full determinant calculations.

2.6 Completing and verifying the algorithm

The cubic estimates require a small margin above Wiener's $1/4$ exponent to absorb logarithmic factors. A separate two-dimensional lattice covers this boundary range; Section 9 gives its cutoff. The remaining dyadic ranges use the component procedures above and finish with fixed-degree elimination and RSA verification.

Combining these steps gives the following proof flow:



In every H_r branch, the second relation lies outside (H_r). Elimination with fixed degrees produces finitely many candidates, and exact RSA verification identifies the target.

3 Preliminaries

3.1 Coefficient norms and Howgrave–Graham

We first define the coefficient norm that converts a short lattice vector into an exact relation at the RSA root. The monomial weights encode the available root bounds, so the determinant calculation and the vanishing test use the same scale.

Definition 3.1 (Scaled coefficient norm)**.** Let $\mathcal{M}$ be a finite set of monomials in variables $v_1, \ldots, v_s$, and let $X_1, \ldots, X_s \geq 1$ be integer bounds. For $M = v^\alpha = v_1^{\alpha_1} \cdots v_s^{\alpha_s}$, write $\mathbf{X}^\alpha = X_1^{\alpha_1} \cdots X_s^{\alpha_s}$. Let $P = \sum_{v^\alpha \in \mathcal{M}} p_\alpha v^\alpha$. For formal variables $z_1, \ldots, z_s$, define

$$\|P\|_{\mathbf{X}} := \|P(X_1 z_1, \ldots, X_s z_s)\|_2 := \left(\sum_{v^\alpha \in \mathcal{M}} (p_\alpha \mathbf{X}^\alpha)^2 \right)^{1/2},$$

where the norm on the middle expression is the Euclidean norm of its coefficient vector. The scaled coefficient vector is therefore

$$\mathrm{coeff}_{\mathbf{X}}(P) = (p_\alpha \mathbf{X}^\alpha)_{M = v^\alpha \in \mathcal{M}}.$$

A coefficient lattice is a lattice generated by such scaled coefficient vectors of integer polynomials.

We identify polynomials with their scaled coefficient vectors. Under this identification, a vector $\mathbf{w} = (w_\alpha)_\alpha$ represents the polynomial $\sum_{v^\alpha \in \mathcal{M}} w_\alpha \mathbf{X}^{-\alpha} v^\alpha$. Euclidean vector norms and orthogonal projections use the scaled coordinates, while evaluation refers to the corresponding polynomial.

If $|v_i^{(0)}| \leq X_i$, Cauchy–Schwarz gives

$$|P(v_1^{(0)}, \ldots, v_s^{(0)})| \leq \sqrt{|\mathcal{M}|}\, \|P\|_{\mathbf{X}}. \tag{4}$$

The evaluation constant is determined by the ambient support size $|\mathcal{M}|$.

Lemma 3.2 (Howgrave–Graham Lemma)**.** *Let $P \in \mathbb{Z}[v_1, \ldots, v_s]$ be supported on $\mathcal{M}$, and let $(v_1^{(0)}, \ldots, v_s^{(0)}) \in \mathbb{Z}^s$ satisfy $|v_i^{(0)}| \leq X_i$. Suppose that*

$$P(v_1^{(0)}, \ldots, v_s^{(0)}) \equiv 0 \pmod{e^m}.$$

If

$$\|P\|_{\mathbf{X}} < \frac{e^m}{\sqrt{|\mathcal{M}|}},$$

then $P(v_1^{(0)}, \ldots, v_s^{(0)}) = 0$ in $\mathbb{Z}$.

Proof. Equation (4) shows that the absolute value is strictly smaller than e^m. It is also an integer multiple of e^m, so it is zero. This is the standard scaled-coefficient form of the Howgrave–Graham lemma [HG97]. □

3.2 Lattices, saturation, and orthogonal quotients

The second relation will be found after removing the known multiples of a factor. We therefore recall the lattice notions needed to form that quotient and to measure its short vectors.

Definition 3.3. Let V be a Euclidean vector space. A *lattice* in V is a discrete subgroup of the form

$$L = \mathbb{Z} b_1 + \cdots + \mathbb{Z} b_r,$$

where $b_1, \ldots, b_r \in V$ are linearly independent. The integer r is the rank of L, and the real span of L is $\mathrm{span}_{\mathbb{R}}\{b_1, \ldots, b_r\}$.

For a rank-r Euclidean lattice L, write $\det L$ for its covolume in its real span and $\lambda_1(L)$ for the length of its shortest nonzero vector. Minkowski's theorem gives

$$\lambda_1(L) \le C_r(\det L)^{1/r}, \tag{5}$$

where C_r depends only on r. All lattice ranks in the proof are fixed independently of N. The largest ambient level lattice has rank 132, but exact SVP is used only in ranks at most 42; the final instance in the low-height cubic branch has rank 31. We use exact SVP for the first relation because shortestness also controls its factorization: in Section 5, it ensures canonical primitivity and, when the y-shift coefficient is zero, excludes a relation with two nonzero homogeneous blocks.

Lemma 3.4. *For every fixed rank r, a shortest nonzero vector of a lattice given by an integral basis can be computed deterministically in time polynomial in the basis bit length. The same holds when the lattice is specified by a rational positive-definite Gram matrix, with complexity measured in the bit length of that matrix.*

Proof. For fixed rank, deterministic exact SVP algorithms [HS07, MV10] run in time polynomial in the input bit length. For a rational Gram matrix, clearing a common denominator of polynomial bit length reduces all inner-product calculations to integral arithmetic. This scales every length by the same factor and preserves the shortest vectors. □

Definition 3.5. Recall that a sublattice $K \subseteq L$ is *saturated*, or *primitive*, in L if $av \in K$, $a \in \mathbb{Z} \setminus \{0\}$, and $v \in L$ imply $v \in K$. Equivalently, L/K is torsion free; equivalently,

$$K = L \cap \operatorname{span}_{\mathbb{Q}} K.$$

Let $K \subseteq L$ be saturated and let π_K be orthogonal projection onto $(\operatorname{span}_{\mathbb{R}} K)^{\perp}$. The *orthogonal quotient lattice* is $Q = L/K := \pi_K(L)$, equipped with the induced Euclidean metric. It is a lattice of rank $\operatorname{rank} L - \operatorname{rank} K$. For a Euclidean lattice Λ, its dual $\Lambda^* = \{\ell \in (\operatorname{span}_{\mathbb{R}} \Lambda)^* : \ell(\Lambda) \subseteq \mathbb{Z}\}$ is equipped with the Riesz dual norm. The norm on $\bigwedge^k (\operatorname{span}_{\mathbb{R}} \Lambda)^*$ is the induced exterior Euclidean norm; equivalently, the squared norm of a row wedge is the sum of the squares of its $k \times k$ minors in any orthonormal basis.

Lemma 3.6. *If $K \subseteq L$ is saturated, then*

$$\det L = (\det K)(\det Q).$$

If L and K are given by rational bases, a rational basis of Q and a preimage in L of each quotient basis vector are computable in polynomial time.

Proof. Saturation permits a $\mathbb{Z}$-basis of K to be extended to a $\mathbb{Z}$-basis of L. In the corresponding basis, Gram–Schmidt first along $\operatorname{span} K$ and then perpendicular to it makes the Gram determinant block triangular. Taking square roots gives the identity. Hermite or Smith normal form finds the extended basis. Orthogonal projection is rational when the input Gram matrix is rational, so the projected basis is computed exactly, and the extended basis gives the required preimages. □

For $\mathbf{v} \in Q$, any $P \in L$ satisfying $\pi_K(P) = \mathbf{v}$ is an *integer preimage* of $\mathbf{v}$. The projected vector $\mathbf{v}$ is generally rational. When the projection kernel vanishes at the target, $\mathbf{v}$ and any integer preimage have the same value there. Thus an integer preimage may be chosen in the proof to certify divisibility, while the algorithm works with $\mathbf{v}$ itself.

Lemma 3.7 (Projected Howgrave–Graham Lemma)**.** *Let L be an integer coefficient lattice supported on $\mathcal{M}$, with the scaled norm induced by coordinate bounds valid at the target root. Suppose every $P \in L$ evaluates to a multiple of e^m there. Let W be a rational polynomial subspace*

whose elements vanish at that root, put $K = L \cap W$*, and let* $Q = \pi_K(L)$*. For every* $\mathbf{v} \in Q$ *and any* $P \in L$ *satisfying* $\pi_K(P) = \mathbf{v}$*,*

$$\mathbf{v}(x_0, u_0, y_0) = P(x_0, u_0, y_0) \in e^m\mathbb{Z}$$

and

$$|\mathbf{v}(x_0, u_0, y_0)| \le \sqrt{|\mathcal{M}|}\,\|\mathbf{v}\|_2.$$

Consequently, if $\mathbf{v} \neq 0$ *and*

$$\|\mathbf{v}\|_2 < \frac{e^m}{\sqrt{|\mathcal{M}|}},$$

then $\mathbf{v}(x_0, u_0, y_0) = 0$ *and* $\mathbf{v} \notin W$*. Clearing denominators gives an integer polynomial with the same two properties.*

Proof. Because W is rational, $\operatorname{span}_{\mathbb{R}}(L \cap W) = \operatorname{span}_{\mathbb{R}} L \cap W$. Evaluation therefore annihilates the projection kernel. Thus $\mathbf{v}$ and any integer preimage P have the same value at the target, and this value belongs to $e^m\mathbb{Z}$. The operator norm of evaluation in the scaled coefficient space is at most $\sqrt{|\mathcal{M}|}$, which proves the bound. The strict estimate and the same divisibility argument as in Lemma 3.2 force this value to be zero. If $\mathbf{v} \in W$, then rationality of W gives $\mathbf{v} \in \operatorname{span}_{\mathbb{R}} K$. Since also $\mathbf{v} \perp \operatorname{span}_{\mathbb{R}} K$, this would imply $\mathbf{v} = 0$. Finally, multiplication by a nonzero common denominator preserves both vanishing and nonmembership in W. □

3.3 The graph ring and level shifts

The graph relation lets us work with integral polynomials while preserving the RSA identity $Ax + u = ed$ at the target. The following ring and level notation packages this relation for the lattice constructions.

Definition 3.8. Set

$$\mathcal{G}_{\mathbb{Z}} = \mathbb{Z}[x, u, y]/(xy - u + 1).$$

The graph normal form $\mathrm{NF}(P)$ is the remainder after repeatedly replacing xy by $u - 1$. Its monomials do not contain both a positive power of x and a positive power of y.

Because the relation is monic in xy, normal form preserves integral coefficients. The substitution $u \mapsto 1 + xy$ gives $\mathcal{G}_{\mathbb{Z}} \simeq \mathbb{Z}[x, y]$, so the graph ring is an integral domain and a unique factorization domain. Put $\mathcal{G}_{\mathbb{Q}} = \mathcal{G}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}$.

Definition 3.9. For $m \ge 1$, a *level-m shift* is a graph-normal integer polynomial whose value at the RSA root is an integer multiple of e^m. A lattice generated over $\mathbb{Z}$ by level shifts is a level lattice.

3.4 Canonical pairs and integral factor lifts

The front relation will be factored in coordinates adapted to its level. Canonical pairs provide those coordinates and, through their integral lift, translate factors back into the graph ring.

Consider an integral graph polynomial of the shape

$$P_m = eA_{m-1}(ex, \bar{f}) + B_m(ex, \bar{f}) + c\,y\bar{f}^m, \tag{6}$$

where A_{m-1} and B_m are integral binary forms of the indicated degrees. In the localization $\mathcal{G}_{\mathbb{Q}}[\bar{f}^{-1}]$, put

$$z = \frac{ex}{\bar{f}}, \qquad a(z) = A_{m-1}(z, 1) \in \mathbb{Z}[z]_{\le m-1}, \qquad b(z) = B_m(z, 1) \in \mathbb{Z}[z]_{\le m}.$$

Thus $a(z)$ and $b(z)$ are dehomogenized one-variable polynomials of the indicated degrees. In the graph ring,

$$u = 1 + xy, \qquad \bar{f} = Ax + u, \qquad z = \frac{ex}{\bar{f}}.$$

Hence

$$\begin{aligned} \bar{f} \cdot (e - Az - zy) &= e\bar{f} - Az\bar{f} - zy\bar{f} \\ &= e(Ax + u) - Aex - exy \\ &= e(u - xy) = e. \end{aligned} \tag{7}$$

After localizing at $\bar{f}$, this gives

$$\frac{e}{\bar{f}} = e - Az - zy. \tag{8}$$

Eliminating $\bar{f}^{-1}$ from (6) gives

$$\frac{P_m}{\bar{f}^m} = C_m(z)y + D_m(z), \quad C_m = c - za(z), \quad D_m = (e - Az)a(z) + b(z). \tag{9}$$

Definition 3.10 (Canonical primitivity)**.** The polynomial (6) is *canonically primitive* if all coefficients of C_m and D_m have greatest common divisor one.

Definition 3.11 (Canonical degree)**.** For a pair $C, D \in \mathbb{Z}[z]$ with $\gcd_{\mathbb{Q}[z]}(C, D) = 1$, the *canonical degree* is

$$\max\{\deg C, \deg D\}.$$

If $H \in \mathcal{G}_{\mathbb{Z}}$, then (H) denotes the rational principal ideal $H\mathcal{G}_{\mathbb{Q}}$. Thus $\mathcal{L}_m \cap (H)$ always means $\mathcal{L}_m \cap H\mathcal{G}_{\mathbb{Q}}$, even when the displayed multiplier module is integral.

Lemma 3.12. *The map*

$$(a(z), b(z), c_0) \longmapsto (C_m, D_m)$$

defined by

$$C_m(z) = c_0 - za(z), \qquad D_m(z) = (e - Az)a(z) + b(z)$$

is a $\mathbb{Z}$-module isomorphism

$$\mathbb{Z}[z]_{\le m-1} \oplus \mathbb{Z}[z]_{\le m} \oplus \mathbb{Z} \longrightarrow \mathbb{Z}[z]_{\le m} \oplus \mathbb{Z}[z]_{\le m}.$$

Its inverse is

$$c_0 = C_m(0), \qquad a(z) = \frac{C_m(0) - C_m(z)}{z}, \qquad b(z) = D_m - (e - Az)a(z). \tag{10}$$

In coefficient bases its determinant is ± 1.

Proof. The numerator $C_m(0) - C_m(z)$ has zero constant coefficient, so division by z is an integral coefficient shift. Substitution verifies both compositions. The inverse uses only integral additions and coefficient shifts, and therefore the matrix is unimodular. □

Lemma 3.13. *Let P_m be canonically primitive and have $c \neq 0$. Normalize $\chi = \gcd_{\mathbb{Z}[z]}(C_m, D_m)$ to be primitive with positive leading coefficient, and write*

$$C_m = \chi C', \qquad D_m = \chi D', \qquad s = \deg \chi, \qquad r = \max(\deg C', \deg D').$$

Then $C', D' \in \mathbb{Z}[z]$, their joint coefficient content is one, and Lemma 3.12 at degree r gives the unique integral graph polynomial with canonical pair (C', D'):

$$H_r = eA'_{r-1}(ex, \bar{f}) + B'_r(ex, \bar{f}) + c'y\bar{f}^r.$$

Moreover, $c' = C'(0) \neq 0$, and for $r \geq 1$, H_r is a level-r shift. For $r = 0$, the notation means $A'_{-1} = 0$ and $H_0 = B'_0 + c'y$. Writing $\widetilde{\chi}(S, T) = T^s\chi(S/T)$, one has the exact identity

$$P_m = \bar{f}^{m-s-r}\widetilde{\chi}(ex, \bar{f})H_r \quad \text{in } \mathcal{G}_{\mathbb{Z}}. \tag{11}$$

Proof. Gauss' lemma gives integral quotients after the primitive normalization of χ. If a prime divided all coefficients of C' and D', then, because χ is nonzero modulo that prime, it would divide every coefficient of C_m, D_m, contrary to canonical primitivity. The inverse map (10) is integral and gives H_r. Since $c = \chi(0)C'(0) \neq 0$, both $\chi(0)$ and $C'(0) = c'$ are nonzero. At the RSA root, both ex_0 and $\bar{f}(x_0, u_0) = ed$ are divisible by e. Every term in $eA'_{r-1}(ex_0, ed)$, $B'_r(ex_0, ed)$, and $c'y_0(ed)^r$ is therefore divisible by e^r. Hence H_r is a level-r shift. Finally, multiply the localized equality $P_m/\bar{f}^m = \chi(C'y + D')$ by $\bar{f}^m$. The definition of homogeneous lift gives exactly (11). The degree inequalities give $m - s - r \geq 0$. □

3.5 Elimination from two coprime relations

For two polynomials $F, G \in \mathbb{Q}[x, y]$, the resultant $\mathrm{Res}_y(F, G)$ is the determinant of the Sylvester matrix. If F, G are coprime, then after at most a fixed linear change of variables one of the two coordinate resultants is nonzero. The ideal (F, G) is then zero dimensional, and every common zero has a coordinate among the roots of a fixed-degree univariate resultant. Factoring the resultant and back-substituting recovers all rational or integer common zeros [CLO15]. For fixed degrees, the Sylvester determinants have fixed size, coefficient bit lengths grow only polynomially, deterministic factorization in $\mathbb{Q}[z]$ is polynomial time [LLL82], and back-substitution has the same polynomial complexity. For each rational resultant root, specialize the two polynomials, compute their univariate gcd, and list its rational roots. For an irreducible first polynomial, coprimality is equivalent to requiring the second polynomial to lie outside its principal ideal.

4 The front rank-eight lattice

We now construct the first relation. The shifts below all retain level-three divisibility at the target. Their scaled coefficient lattice is small enough below the 11/42 threshold to yield the first exact relation.

Consider the graph-reduced integer polynomials

$$\mathcal{S}_3 = \{e^3x^2,\ e^2x\bar{f},\ e\bar{f}^2, e^3x^3,\ e^2x^2\bar{f},\ ex\bar{f}^2, \bar{f}^3,\ \mathrm{NF}(y\bar{f}^3)\}. \tag{12}$$

At the target root,

$$e^{3-k}x_0^i\bar{f}(x_0, u_0)^k = e^3x_0^id^k, \qquad \mathrm{NF}(y\bar{f}^3)(x_0, u_0, y_0) = e^3y_0d^3.$$

The first identity is used only for the exponents that occur in the first seven shifts in (12). Therefore every integer combination of the rows evaluates to a multiple of e^3. This gives the Howgrave–Graham divisibility needed below.

The graph reduction of the y-shift is

$$\begin{aligned}\mathrm{NF}(y\bar{f}^3) &= yu^3 + (u-1)(3Au^2 + 3A^2xu + A^3x^2)\\ &= -A^3x^2 - 3A^2xu - 3Au^2 + A^3x^2u + 3A^2xu^2 + 3Au^3 + yu^3.\end{aligned} \tag{13}$$

Every row under consideration already has zero coefficient on $1, x, u$. Removing these three identically zero coordinates is therefore an isometric identification of the row lattice.

Lemma 4.1. *Let L_3 be the coefficient lattice of the rows in* (12)*, in the column order*

$$(x^2, xu, u^2, x^3, x^2u, xu^2, u^3, yu^3).$$

Then L_3 has rank eight and

$$\det L_3 = e^{12}X^9YU^{12}.$$

For every fixed $\eta > 0$, if $X \leq e^{11/42-\eta}$, then, for all sufficiently large N, exact SVP in L_3 returns a nonzero integer polynomial P_3 with $P_3(x_0, u_0, y_0) = 0$ over $\mathbb{Z}$.

Proof. Shift polynomials label rows, scaled monomials label columns, and coefficient vectors are row vectors. The complete scaled coefficient matrix is

$$\begin{array}{c} \\ e^3x^2 \\ e^2x\bar{f} \\ e\bar{f}^2 \\ e^3x^3 \\ e^2x^2\bar{f} \\ ex\bar{f}^2 \\ \bar{f}^3 \\ \mathrm{NF}(y\bar{f}^3) \end{array} \begin{array}{c} \begin{array}{cccccccc} x^2 & xu & u^2 & x^3 & x^2u & xu^2 & u^3 & yu^3 \end{array} \\ \begin{pmatrix} e^3X^2 & & & & & & & \\ e^2AX^2 & e^2XU & & & & & & \\ eA^2X^2 & 2eAXU & eU^2 & & & & & \\ & & & e^3X^3 & & & & \\ & & & e^2AX^3 & e^2X^2U & & & \\ & & & eA^2X^3 & 2eAX^2U & eXU^2 & & \\ & & & A^3X^3 & 3A^2X^2U & 3AXU^2 & U^3 & \\ -A^3X^2 & -3A^2XU & -3AU^2 & & A^3X^2U & 3A^2XU^2 & 3AU^3 & YU^3 \end{pmatrix} \end{array}.$$

It is lower triangular in the displayed order. Hence

$$\begin{aligned} \det L_3 &= (e^3X^2)(e^2XU)(eU^2)(e^3X^3)(e^2X^2U)(eXU^2)(U^3)(YU^3) \\ &= e^{12}X^9YU^{12}. \end{aligned} \tag{14}$$

Write $\delta = \log_e X$. Since $e = \Theta(N)$, we have $\log_e Y = 1/2 + O(1/\log e)$, and $U = XY$. Consequently,

$$\log_e \det L_3 = 12 + 9\delta + \frac{1}{2} + 12\left(\delta + \frac{1}{2}\right) + O(1/\log e) = \frac{37}{2} + 21\delta + O(1/\log e). \tag{15}$$

To obtain a vector of length below a constant multiple of e^3 in rank eight, we compare the determinant exponent with $3 \cdot 8 = 24$:

$$\frac{37}{2} + 21\delta < 24 \quad \Longleftrightarrow \quad \delta < \frac{11}{42}.$$

Equivalently, with $\delta = 1/4 + \theta$, this is $\theta < 1/84$.

If $\delta \le 11/42 - \eta$, then $\det L_3 \le e^{24-10\eta}$, say, for all sufficiently large N. Equation (5) now gives

$$\lambda_1(L_3) \le C_8 e^{3-(5/4)\eta} < \frac{e^3}{\sqrt{8}}$$

for sufficiently large N. Exact fixed-dimensional SVP returns an integer combination of the eight rows. Its support has eight monomials, its value is divisible by e^3, and Lemma 3.2 proves that its value is zero. □

Remark 4.2. The front lattice remains unsaturated so that level-three divisibility is preserved.

If $d \le N^{11/42-\varepsilon}$ and X is the upper endpoint of the correct dyadic range, then $X < 2d$. Since $e = \Theta(N)$, for sufficiently large N,

$$\log_e X \le \frac{11}{42} - \frac{\varepsilon}{2}. \tag{16}$$

Thus Lemma 4.1 has a fixed power saving depending on ε.

5 Classification of the first exact relation

The first exact relation reduces root recovery to a fixed number of cases. Some factors determine the key directly; the remaining factors have canonical degree one, two, or three. The next proposition gives the list that the algorithm will examine.

Every $P_3 \in L_3$ has a unique expression

$$P_3 = eA_2(ex, \bar{f}) + B_3(ex, \bar{f}) + c\,y\bar{f}^3, \tag{17}$$

with integral binary forms A_2, B_3.

Proposition 5.1 (Component classification)**.** *Let P_3 be a shortest nonzero vector of L_3, and suppose that $P_3(x_0, u_0, y_0) = 0$. From P_3, one can compute a list of equations of the following types:*

(i) a nonzero univariate equation in z, of degree at most three;

(ii) an equation $H_0 = B_0' + c'y = 0$, where $c' \neq 0$;

(iii) an equation $H_r = 0$ for $r \in \{1, 2, 3\}$, where H_r is a canonically primitive integral graph polynomial, irreducible in $\mathcal{G}_{\mathbb{Q}}$, of exact canonical degree r, and with nonzero $y\bar{f}^r$-coefficient.

The list has bounded size and is computable in time polynomial in the coefficient bit length. At least one equation is satisfied at the RSA root, with $z = x_0/d$. In case (i)*, its positive rational roots give candidates for (x_0, d) by taking reduced numerators and denominators. In case* (ii)*, the equation determines a candidate for y_0 and hence for $p + q = -y_0$. Only case* (iii) *requires a second relation.*

Proof. Fix the sign of P_3 by requiring the first nonzero entry in the ordered list of coefficients of C_3, followed by those of D_3, to be positive. Shortestness makes its pair canonically primitive: otherwise the unimodular inverse in Lemma 3.12 would divide P_3 by a common integer and produce a strictly shorter nonzero vector of the same lattice.

If $c = 0$, the quadratic and cubic blocks of (17) have disjoint coefficient support. If both were nonzero, either block alone would be a shorter nonzero lattice vector. Hence exactly one block is nonzero. Dividing its equality at the target by the nonzero power of $\bar{f}(x_0, u_0) = ed$ gives a fixed-degree equation in

$$z_0 = \frac{ex_0}{\bar{f}(x_0, u_0)} = \frac{x_0}{d}. \tag{18}$$

Deterministic factorization in $\mathbb{Q}[z]$ lists the linear factors in time polynomial in the coefficient bit length [LLL82]. The RSA root occurs among these rational roots. By (2), its reduced numerator and denominator are (x_0, d).

Suppose $c \neq 0$. Apply Lemma 3.13 to the canonical pair. If $\chi(z_0) = 0$, an irreducible factor of χ having the rational root z_0 is linear and again recovers (x_0, d). Otherwise the exact identity (11) implies that the normalized factor H_r vanishes at the target.

For the remaining factor write

$$\frac{H_r}{\bar{f}^r} = C'(z)y + D'(z).$$

Here $C'(0) \neq 0$ and $\gcd(C', D') = 1$. Therefore $h = C'y + D'$ is irreducible in $\mathbb{Q}[z, y]$. The localization (8), with $\ell = e - Az - zy$, identifies $\mathcal{G}_{\mathbb{Q}}[\bar{f}^{-1}]$ with the localization of $\mathbb{Q}[z, y]$ obtained by inverting ℓ. The polynomial h is not associated to ℓ: its y-coefficient has nonzero constant term, whereas that of ℓ is $-z$. Thus h, and hence H_r, remains irreducible after localization.

We now descend this irreducibility to the rational graph ring. If $r = 0$, then $H_0 = B_0' + c'y$ is linear in y, with $c' \neq 0$, and is already irreducible. Assume $r \geq 1$ below. The graph ring $\mathcal{G}_{\mathbb{Q}} \simeq \mathbb{Q}[x, y]$ is a UFD, and $\bar{f} = 1 + x(A + y)$ is primitive and linear in x, hence irreducible and prime. Put $s = ex$. If a_{r-1} and b_r denote the coefficients of s^{r-1} and s^r in the two homogeneous blocks of H_r, exact canonical degree r says that they are not both zero. Modulo $\bar{f}$,

$$H_r \equiv s^{r-1}(ea_{r-1} + b_r s).$$

The quotient by $(\bar{f})$ identifies with $\mathbb{Q}[x, x^{-1}]$, with $s = ex$, so this residue is nonzero. Therefore $\bar{f} \nmid H_r$. The only units of $\mathcal{G}_{\mathbb{Q}}[\bar{f}^{-1}]$ are $c\bar{f}^n$, with $c \in \mathbb{Q}^\times$ and $n \in \mathbb{Z}$. If H_r factored in $\mathcal{G}_{\mathbb{Q}}$, localization would make one factor such a unit. UFD factorization and $\bar{f} \nmid H_r$ make that factor a constant. Hence H_r is irreducible already in the rational graph ring.

When $c \neq 0$, the algorithm lists the nonconstant common-factor equation $\chi(z) = 0$, if present, together with $H_r = 0$; it need not know which one contains the target. The factorization identity ensures that one does. Since $r \leq 3$, this gives exactly the stated types. The canonical inverse, gcd computation, and univariate factorization all have fixed degree and polynomial bit complexity. For $r = 0$, the equation $B'_0 + c'y = 0$ directly determines the candidate prime sum. □

6 The level lattices

The remaining factors need a second relation. We construct level lattices whose generators evaluate to multiples of e^m at the RSA root. Two coordinate maps serve different purposes: the formal lift ν_m records evaluation after removing this factor e^m, while the localized map Φ_m identifies the lattice with an integral rectangular coefficient module. The latter lets us compute the exact intersection with the multiples of a known factor H_r. Lengths and determinants are always measured in the original weighted coefficient space; these coordinate maps are algebraic identifications.

For $m \geq 1$, let $\mathcal{L}_m$ be the coefficient lattice generated, after graph normal form, by

$$G_{n,i} = e^{m-n}(ex)^i \bar{f}^{\,n-i}, \qquad 1 \leq n \leq m, \quad 0 \leq i \leq n, \tag{19}$$

$$G^{(y)}_{k,j} = e^{m-k} y^j \bar{f}^k, \qquad 2 \leq k \leq m, \quad 1 \leq j < k. \tag{20}$$

At the target root,

$$G_{n,i}(x_0, u_0, y_0) = e^m x_0^i d^{n-i}, \qquad G^{(y)}_{k,j}(x_0, u_0, y_0) = e^m y_0^j d^k. \tag{21}$$

In particular, $\mathcal{L}_3$ is the level-three lattice of rank twelve. It contains the rank-eight front lattice L_3 used to construct the first relation.

Lemma 6.1. *The rows* (19)–(20) *are linearly independent and*

$$\operatorname{rank} \mathcal{L}_m = m(m+1). \tag{22}$$

Their weighted determinant is

$$\det \mathcal{L}_m = e^{m^2(m+1)/2} X^{m(m+1)(m+2)/6} U^{m^2(m+1)/2} Y^{m(m+1)(m-1)/6}. \tag{23}$$

There is a $\mathbb{Z}$-linear map $\nu_m : \mathcal{L}_m \to \mathbb{Z}[x, d, y]$, where x, d, y are formal variables. It is defined on the row basis by

$$\nu_m(G_{n,i}) = x^i d^{n-i}, \qquad \nu_m(G^{(y)}_{k,j}) = y^j d^k, \tag{24}$$

Evaluation substitutes the RSA private exponent for the formal variable d. For every $P \in \mathcal{L}_m$,

$$P(x_0, u_0, y_0) = e^m \nu_m(P)(x_0, d, y_0). \tag{25}$$

In particular, $\nu_m(P)(x_0, d, y_0) \in \mathbb{Z}$.

Proof. Order the normal monomials first by the pure blocks $x^i u^{n-i}$, and then by $y^j u^k$. The distinguished coefficient of $G_{n,i}$ is

$$e^{m-n+i} x^i u^{n-i},$$

whereas the distinguished coefficient of $G^{(y)}_{k,j}$ is $e^{m-k} y^j u^k$. All other terms precede the distinguished term in the corresponding block order. Thus the matrix is triangular. Counting rows gives

$$\sum_{n=1}^{m} (n+1) + \sum_{k=2}^{m} (k-1) = m(m+1).$$

Multiplication of the diagonal entries gives the exponent sums

$$\sum_{n=1}^{m}\sum_{i=0}^{n}(m-n+i)+\sum_{k=2}^{m}\sum_{j=1}^{k-1}(m-k)=\frac{m^2(m+1)}{2},$$

$$\sum_{n=1}^{m}\sum_{i=0}^{n} i=\frac{m(m+1)(m+2)}{6},$$

$$\sum_{n=1}^{m}\sum_{i=0}^{n}(n-i)+\sum_{k=2}^{m}\sum_{j=1}^{k-1} k=\frac{m^2(m+1)}{2},$$

$$\sum_{k=2}^{m}\sum_{j=1}^{k-1} j=\frac{m(m+1)(m-1)}{6}.$$

This proves (23). The rows are a $\mathbb{Z}$-basis, so (24) defines a unique $\mathbb{Z}$-linear map. Equation (25) is exactly (21), extended linearly. □

We now introduce the second map, Φ_m, to describe multiples of a factor by ordinary polynomial divisibility. Put $s = ex$, $t = \bar{f}$, and, in the localization at t, put

$$z = s/t, \qquad \ell = e/t = e - Az - zy.$$

For $a, b \geq 0$, write

$$\mathcal{V}^{\mathbb{Z}}_{a,b} = \{P \in \mathbb{Z}[z,y] : \deg_z P \leq a,\ \deg_y P \leq b\}.$$

Lemma 6.2. *For every $m \geq 1$, the map*

$$\Phi_m : \mathcal{L}_m \longrightarrow \mathcal{V}^{\mathbb{Z}}_{m,m-1}, \qquad \Phi_m(P) = P/t^m,$$

is a unimodular $\mathbb{Z}$-module isomorphism.

Proof. On the distinguished basis of Lemma 6.1,

$$\Phi_m(G_{n,i}) = \ell^{m-n} z^i,$$
$$\Phi_m(G^{(y)}_{k,j}) = \ell^{m-k} y^j.$$

Order target monomials by decreasing y-degree and then by z-degree. The first family has distinguished term

$$(-1)^{m-n} z^{i+m-n} y^{m-n}.$$

Writing $a = i + m - n$ and $b = m - n$, these terms cover exactly

$$0 \leq b \leq m-1, \qquad b \leq a \leq m.$$

The second family has distinguished term

$$(-1)^{m-k} z^{m-k} y^{m-k+j};$$

with $a = m - k$ and $b = m - k + j$, it covers exactly

$$0 \leq a < b \leq m-1.$$

The two regions partition the rectangle $0 \leq a \leq m,\ 0 \leq b \leq m-1$. Every other term has smaller y-degree, and every distinguished coefficient is ± 1. The change-of-basis matrix is therefore integral triangular with determinant ± 1. □

Corollary 6.3. *Let $H_r \in \mathcal{G}_{\mathbb{Z}}$ satisfy*

$$h_r := H_r/t^r = C(z)y + D(z), \qquad C(0) \neq 0, \qquad \gcd_{\mathbb{Z}[z]}(C, D) = 1, \qquad \max\{\deg C, \deg D\} = r,$$

and suppose that the joint coefficients of C, D are primitive. For $m \geq \max\{r, 2\}$,

$$\Phi_m\big(\mathcal{L}_m \cap (H_r)\big) = h_r \mathcal{V}^{\mathbb{Z}}_{m-r,m-2}. \tag{26}$$

In particular, the intersection is saturated in $\mathcal{L}_m$.

Proof. The polynomial $\ell = e - Az - zy$ is irreducible in $\mathbb{Q}[z, y]$. The primitive y-linear polynomial h_r is also irreducible. They cannot be associates: the coefficient of y in h_r has nonzero constant term, whereas that of ℓ is $-z$. Hence $\gcd(h_r, \ell) = 1$.

If $P \in \mathcal{L}_m \cap (H_r)$, divisibility in the localized rational graph ring initially gives $h_r \mid \ell^v \Phi_m(P)$ in $\mathbb{Q}[z, y]$ for some $v \geq 0$. Euclid's lemma removes ℓ^v. Write $\Phi_m(P) = h_r Q$. Additivity of degrees in the domains $\mathbb{Q}[z][y]$ and $\mathbb{Q}[y][z]$ gives

$$\deg_y Q \leq m - 2, \qquad \deg_z Q \leq m - r.$$

Gauss' lemma and primitivity of h_r give $Q \in \mathbb{Z}[z, y]$. Conversely, every such product lies in the target rectangle and hence, by Lemma 6.2, has a unique integral preimage in $\mathcal{L}_m$. Multiplying by t^m shows that this preimage is divisible by $H_r = t^r h_r$. This proves (26). Finally, the right side is the intersection of the ambient integer module with a rational subspace, so its inverse image is saturated. □

7 The linear and quadratic cases

For canonical degrees $r = 1$ and $r = 2$, a low level already supplies the needed second relation. Both cases follow the same argument. We compute the saturated intersection $\mathcal{L}_m \cap (H_r)$, bound its covolume by an explicit minor, and divide the ambient determinant by this bound. A shortest nonzero vector in the resulting quotient then satisfies Lemma 3.7.

The common recovery step is as follows. Projected Howgrave–Graham gives a rational polynomial that vanishes at the target and lies outside (H_r). Clearing denominators preserves both properties. Since $\mathcal{G}_{\mathbb{Q}} \simeq \mathbb{Q}[x, y]$ and H_r is irreducible, the two polynomials are coprime. Fixed-degree elimination then lists the candidates for exact RSA verification.

The two constructions use the following parameters; the lemmas below state the corresponding bounds with a fixed margin.

Factor	Level	Quotient rank	Exponent range
H_1	2	4	$\delta < 1/3$
H_2	3	8	$\delta < 9/34$

Both ranges contain the target range because $11/42 < 9/34 < 1/3$.

7.1 The linear case

Let

$$H_1 = e\alpha + \beta(ex) + \gamma\bar{f} + c\,y\bar{f}, \qquad c \neq 0, \tag{27}$$

be a known canonically primitive irreducible factor that vanishes at the target root and has exact canonical degree one.

Lemma 7.1. *Let H_1 have the form (27). Suppose that it is canonically primitive, irreducible in $\mathcal{G}_{\mathbb{Q}}$, of exact canonical degree one, and vanishes at the target root. Then:*

(i) The saturated intersection in $\mathcal{L}_2$ is

$$\mathcal{L}_2 \cap (H_1) = \mathbb{Z}(ex)H_1 \oplus \mathbb{Z}\bar{f}H_1. \tag{28}$$

(ii) The orthogonal quotient Q_{H_1} has rank four and satisfies

$$\det Q_{H_1} \le e^5 X^4 U^2. \tag{29}$$

(iii) For every fixed $\eta > 0$, if $X \le e^{1/3-\eta}$, then for all sufficiently large N, the quotient contains a nonzero vector that vanishes at the target and lies outside (H_1).

Proof. Put $s = ex$ and $t = \bar{f}$. Relative to the basis

$$(es, et, s^2, st, t^2, yt^2)$$

of $\mathcal{L}_2$, the columns of sH_1, tH_1 are

$$M_1 = \begin{pmatrix} \alpha & 0 \\ -c & \alpha \\ \beta & 0 \\ \gamma - cA & \beta \\ ce & \gamma \\ 0 & c \end{pmatrix}. \tag{30}$$

Here we use the integral graph identity

$$sy = et - As - e. \tag{31}$$

In the localized coordinates of Corollary 6.3,

$$h := H_1/t = C_1(z)y + D_1(z), \quad C_1 = c - \alpha z, \quad D_1 = e\alpha + \gamma + (\beta - A\alpha)z.$$

The hypotheses on H_1 say precisely that C_1, D_1 are jointly primitive and coprime, $C_1(0) = c \neq 0$, and $\max\{\deg C_1, \deg D_1\} = 1$. Corollary 6.3 with $(m, r) = (2, 1)$ therefore gives

$$\Phi_2\big(\mathcal{L}_2 \cap (H_1)\big) = h\mathcal{V}_{1,0}^{\mathbb{Z}} = h\langle 1, z\rangle_{\mathbb{Z}}.$$

Multiplication by t^2 turns the two cofactors into t, s, proving (28) integrally and proving saturation.

Lemma 6.1 gives

$$\det \mathcal{L}_2 = e^6 X^4 U^6 Y.$$

In graph-normal weighted coordinates, the rows u^2, yu^2 of the two product columns have determinant $c^2 eYU^4$. Cauchy–Binet therefore gives

$$\det(\mathcal{L}_2 \cap (H_1)) \ge |c|^2 eYU^4 \ge eYU^4.$$

Lemma 3.6 proves (29).

If $X = e^{\delta}$, then $U = e^{\delta + 1/2 + O(1/\log e)}$, so

$$\log_e \det Q_{H_1} \le 6 + 6\delta + O(1/\log e).$$

For $\delta \le 1/3 - \eta$, apply Lemma 3.7 with $W = (H_1) \cap \operatorname{span}_{\mathbb{Q}} \mathcal{L}_2$. Minkowski in quotient rank four gives

$$\lambda_1(Q_{H_1}) \le C_4 (\det Q_{H_1})^{1/4} \le C_4 e^{3/2 + (3/2)\delta + O(1/\log e)} \le C_4 e^{2 - (3/2)\eta + O(1/\log e)}.$$

For sufficiently large N, this is strictly smaller than $e^2/\sqrt{6}$, the level-two bound for the six coefficient coordinates of $\mathcal{L}_2$. Lemma 3.7 therefore gives vanishing at the target and nonmembership in (H_1), as claimed. □

7.2 The quadratic case

Put $s = ex$ and $t = \bar{f}$, and write H_2 as

$$H_2 = e(\alpha s + \beta t) + \gamma s^2 + \lambda st + \eta t^2 + c\, y t^2, \qquad c \neq 0. \tag{32}$$

Let this be a known canonically primitive irreducible factor that vanishes at the target and has canonical degree exactly two.

Lemma 7.2. *Let H_2 have the form (32). Suppose that it is canonically primitive, irreducible in $\mathcal{G}_{\mathbb{Q}}$, of exact canonical degree two, and vanishes at the target root. Then:*

(i) The saturated intersection in $\mathcal{L}_3$ is

$$\mathcal{L}_3 \cap (H_2) = H_2 \langle e, ex, \bar{f}, y\bar{f} \rangle_{\mathbb{Z}}. \tag{33}$$

(ii) The orthogonal quotient Q_{H_2} has rank eight and satisfies

$$\det Q_{H_2} \leq e^{16} X^{10} U^7. \tag{34}$$

(iii) For every fixed $\eta_0 > 0$, if $X \leq e^{9/34-\eta_0}$, then for all sufficiently large N, the quotient contains a nonzero vector that vanishes at the target and lies outside (H_2).

Proof. Use the ordered basis

$$\mathcal{B}_3 = (e^2 s, e^2 t, es^2, est, et^2, s^3, s^2 t, st^2, t^3, eyt^2, yt^3, y^2 t^3)$$

of $\mathcal{L}_3$. Repeated use of $sy = et - As - e$ gives the complete coordinate matrix whose columns are eH_2, sH_2, tH_2, ytH_2. Split its rows after the sixth basis vector and write $M_2 = \left(\begin{smallmatrix} M_2^{\mathrm{top}} \\ M_2^{\mathrm{bot}} \end{smallmatrix}\right)$. Its two six-row blocks are

$$M_2^{\mathrm{top}} = \begin{pmatrix} \alpha & 0 & 0 & 0 \\ \beta & 0 & 0 & -\alpha \\ \gamma & \alpha & 0 & 0 \\ \lambda & \beta & \alpha & -A\alpha - \gamma \\ \eta & -c & \beta & e\alpha - \lambda \\ 0 & \gamma & 0 & 0 \end{pmatrix} \qquad \text{and} \qquad M_2^{\mathrm{bot}} = \begin{pmatrix} 0 & \lambda & \gamma & -A\gamma \\ 0 & \eta - Ac & \lambda & e\gamma - A\lambda \\ 0 & ec & \eta & e\lambda \\ c & 0 & 0 & \beta \\ 0 & 0 & c & \eta \\ 0 & 0 & 0 & c \end{pmatrix}. \tag{35}$$

For example,

$$\gamma s^2 yt = e\gamma st^2 - A\gamma s^2 t - e\gamma st, \qquad \lambda syt^2 = e\lambda t^3 - A\lambda st^2 - e\lambda t^2.$$

On the localized chart,

$$H_2/t^2 = h(z, y) = C(z)y + D(z),$$

where

$$C(z) = c - \beta z - \alpha z^2, \tag{36}$$

$$D(z) = e\beta + \eta + (e\alpha - A\beta + \lambda)z + (\gamma - A\alpha)z^2. \tag{37}$$

Canonical primitivity and irreducibility give joint primitivity and $\gcd(C, D) = 1$. A nonconstant common factor would factor $h = Cy + D$ on the localized chart and hence, by the descent argument in Section 5, would factor H_2 in $\mathcal{G}_{\mathbb{Q}}$, contradicting its irreducibility. Exact canonical degree two gives

$$\max(\deg C, \deg D) = 2. \tag{38}$$

Also $C(0) = c \neq 0$. Corollary 6.3 with $(m, r) = (3, 2)$ gives

$$\Phi_3\big(\mathcal{L}_3 \cap (H_2)\big) = h\mathcal{V}_{1,1}^{\mathbb{Z}} = h\langle 1, z, y, zy\rangle_{\mathbb{Z}}.$$

After multiplication by t^3, its multiplier module is $\langle t, s, yt, sy\rangle_{\mathbb{Z}}$. Since $sy = et - As - e$, this equals $\langle e, s, t, yt\rangle_{\mathbb{Z}}$, proving (33) integrally and proving saturation.

For the covolume, order the columns as sH_2, eH_2, tH_2, ytH_2 and select graph-normal monomials u^3, yu^2, yu^3, y^2u^3. The unweighted graph-normal coefficient matrix is

$$\begin{pmatrix} ce & 0 & \eta + 3Ac & e\lambda + 3A\eta + 3A^2c \\ 0 & ce & 0 & e\beta - 3Ac \\ 0 & 0 & c & \eta + 3Ac \\ 0 & 0 & 0 & c \end{pmatrix}.$$

It is upper triangular with determinant c^4e^2. Hence the weighted minor has absolute value

$$|c|^4 e^2 Y^4 U^{11} \geq e^2 Y^4 U^{11}.$$

Since

$$\det \mathcal{L}_3 = e^{18} X^{10} U^{18} Y^4,$$

Lemma 3.6 proves (34).

Finally, apply projected certification with $W = (H_2) \cap \operatorname{span}_{\mathbb{Q}} \mathcal{L}_3$. Then

$$\log_e \det Q_{H_2} \leq \frac{39}{2} + 17\delta + O(1/\log e).$$

If $\delta \leq 9/34 - \eta_0$, Minkowski in quotient rank eight gives

$$\lambda_1(Q_{H_2}) \leq C_8 (\det Q_{H_2})^{1/8} \leq C_8 e^{39/16 + (17/8)\delta + O(1/\log e)} \leq C_8 e^{3 - (17/8)\eta_0 + O(1/\log e)}.$$

For sufficiently large N, this is strictly smaller than $e^3/\sqrt{12}$, the level-three projected-HG bound for the twelve coefficient coordinates of $\mathcal{L}_3$. Lemma 3.7 gives the required relation outside (H_2). □

8 The cubic case

Overview. Our goal is to construct a second relation that vanishes at the RSA root but is not divisible by H_3. We split the argument according to the weighted height of this factor. A large height increases the covolume of the known multiples of H_3 and decreases the quotient determinant, so the direct quotient argument supplies the required relation. For a factor of smaller height, we impose vanishing of the first eleven Taylor coefficients after restriction to the cubic curve. These integral *jet conditions* define a smaller lattice. A short vector in this lattice gives an integer at the RSA root whose upper bound is smaller than its possible nonzero values, forcing it to vanish.

The argument proceeds from the restriction kernel to the two determinant bounds, then to the integer identity and the choice of Taylor expansion point. The notation below records the objects used in these steps; Proposition 8.11 collects their success conditions.

symbol	role
H_3	fixed irreducible cubic factor
f, g, r	one-variable polynomials giving $y = g/f,\ d = f/r,\ x = zf/r$
F, G, R	homogeneous binary forms attached to f, g, r
$\mathcal{R}_m$	restriction of level-m lifts to the cubic curve
K_m	$H_3\mathcal{M}^+_{m-3} = \ker_{\mathbb{Z}} \mathcal{R}_m$
Q_m	$\mathcal{L}_m/K_m$ with the orthogonal quotient metric
$\mathsf{V}(H_3)$	weighted graph-normal height of the cubic
θ, ω_3	$X = e^{1/4+\theta},\ \mathsf{V}(H_3) = e^{11/4-\theta+\omega_3}$
$\lambda_{j,t}$	Taylor row at the chart $z = -j$
γ_j, η_j	$\gamma_j = \gcd(f(-j), g(-j)),\ \eta_j = \log_e \gamma_j$

8.1 Parametrization and formal restriction

We first parametrize the cubic and identify the level polynomials that vanish identically on it. This identifies the exact sublattice to remove before searching for a second relation.

Let $\mathrm{Sym}^D(\mathbb{Z}^2)$ denote the integral binary forms of degree D in variables Z, D_0.

Definition 8.1 (Restriction map)**.** Let V be a finite-dimensional polynomial space and let C be an algebraic curve with a rational parametrization. A *restriction map* is the linear map obtained by substituting the parametrization into elements of V and multiplying by a fixed nonzero rational factor that makes every resulting expression polynomial. Its kernel is the subspace of elements of V vanishing identically on C.

For the cubic calculation, write

$$\sigma = ex, \qquad \tau = \bar{f}.$$

Let

$$H_3 = eA_2(\sigma, \tau) + B_3(\sigma, \tau) + c\, y\tau^3, \qquad c \neq 0, \tag{39}$$

be the fixed canonically primitive normalization of an irreducible factor that vanishes at the target and has canonical degree exactly three. With

$$a(z) = A_2(z, 1) \in \mathbb{Z}[z]_{\leq 2}, \qquad b(z) = B_3(z, 1) \in \mathbb{Z}[z]_{\leq 3},$$

put

$$f(z) = c - za(z), \qquad g(z) = -(e - Az)a(z) - b(z), \qquad r(z) = (e - Az)f(z) - zg(z). \tag{40}$$

Then

$$\gcd_{\mathbb{Q}[z]}(f, g) = 1, \qquad \max(\deg f, \deg g) = 3.$$

On the chart $\tau \neq 0$, and in particular at the target, the canonical equation is $fy = g$. At the target, $f(z_0) \neq 0$, since otherwise $g(z_0) = 0$, contradicting coprimality. Combining $y = g/f$ with the localized graph equation gives

$$y = \frac{g(z)}{f(z)}, \qquad d = \frac{f(z)}{r(z)}, \qquad x = \frac{zf(z)}{r(z)}. \tag{41}$$

In particular $r(z_0) \neq 0$.

Define binary forms of formal degrees $3, 3, 4$ by

$$F(Z, D_0) = D_0^3 f(Z/D_0), \quad G(Z, D_0) = D_0^3 g(Z/D_0), \quad R(Z, D_0) = D_0^4 r(Z/D_0). \tag{42}$$

For $m \geq 3$, define the cofactor module

$$\begin{aligned}\mathcal{M}_{m-3}^{+} = \big\langle & e^{m-3-n}\sigma^{i}\tau^{n-i} \quad (0 \leq n \leq m-3,\ 0 \leq i \leq n), \\ & e^{m-3-k}y^{j}\tau^{k} \quad (0 \leq k \leq m-3,\ 1 \leq j \leq k+1)\big\rangle_{\mathbb{Z}}.\end{aligned} \tag{43}$$

Direct counting gives

$$n_m := \operatorname{rank}\mathcal{L}_m = m(m+1), \qquad \kappa_m := \operatorname{rank}\mathcal{M}_{m-3}^{+} = (m-2)(m-1), \tag{44}$$

and their difference is

$$\varrho_m := n_m - \kappa_m = 4m-2. \tag{45}$$

Recall from Lemma 6.1 that $\nu_m : \mathcal{L}_m \to \mathbb{Z}[x,d,y]$ denotes the formal lift obtained after dividing target evaluations by e^m. To restrict such a lift to the cubic curve, substitute the rational parametrization, multiply by a common denominator, and homogenize. The result is an integral binary form of one fixed degree:

$$\mathcal{R}_m : \nu_m(\mathcal{L}_m) \longrightarrow \operatorname{Sym}^{4m-3}(\mathbb{Z}^2).$$

The binary forms F, G, R supply the common denominator in this construction. On the formal monomials in (24), define

$$\mathcal{R}_m(x^a d^b) = Z^a D_0^b F^{a+b-1} R^{m-a-b}, \tag{46}$$

$$\mathcal{R}_m(y^j d^k) = D_0^k G^j F^{k-j-1} R^{m-k}. \tag{47}$$

All exponents are nonnegative on the distinguished level basis, and both expressions have degree $4m-3$. For instance,

$$a+b+3(a+b-1)+4(m-a-b) = 4m-3.$$

After setting $D_0 = 1$, these formulas equal the parametrized monomial multiplied by $r(z)^m/f(z)$. Thus $\mathcal{R}_m$ is the integral restriction map associated with the rational cubic curve. We use the same symbol for the composition

$$\mathcal{L}_m \xrightarrow{\nu_m} \mathbb{Z}[x,d,y] \xrightarrow{\mathcal{R}_m} \operatorname{Sym}^{4m-3}(\mathbb{Z}^2).$$

Thus $\mathcal{R}_m(P)$ is obtained by applying ν_m, substituting $x = zf/r$, $d = f/r$, and $y = g/f$, multiplying by $r(z)^m/f(z)$, and homogenizing to degree $4m-3$ in (Z, D_0).

Lemma 8.2. *For every H_3 satisfying the hypotheses above and every $m \geq 3$, the restriction map has the following three properties:*

1. $\ker_{\mathbb{Z}} \mathcal{R}_m = H_3\mathcal{M}_{m-3}^{+}$;
2. *this kernel is saturated in $\mathcal{L}_m$;*
3. *the image of $\mathcal{R}_m$ has finite index in $\operatorname{Sym}^{4m-3}(\mathbb{Z}^2)$, equivalently*

$$\mathcal{R}_m \otimes \mathbb{Q} : \mathcal{L}_m \otimes \mathbb{Q} \twoheadrightarrow \operatorname{Sym}^{4m-3}(\mathbb{Q}^2)$$

is surjective.

Proof. We first identify the integral kernel of restriction to the cubic curve. After that, the rank and finite index claims follow from the resulting description of the image. Since

$$\Phi_3(H_3) = f(z)y - g(z), \qquad f(0) = c \neq 0,$$

Corollary 6.3 applies. It gives

$$\Phi_m\big(\mathcal{L}_m \cap (H_3)\big) = (fy-g)\mathcal{V}_{m-3,m-2}^{\mathbb{Z}}.$$

The normalized pure cofactors in (43) are $\ell^{m-3-n}z^i$. Their distinguished monomials cover

$$0 \le b \le a \le m-3.$$

The normalized y-cofactors are $\ell^{m-3-k}y^j$. Their distinguished monomials cover

$$0 \le a < b \le m-2, \qquad a \le m-3.$$

Together these regions are the whole rectangle $\mathcal{V}^{\mathbb{Z}}_{m-3,m-2}$, without repetition, and every pivot is ± 1. Thus the displayed cofactors form a unimodular basis of that rectangle. Consequently

$$\mathcal{L}_m \cap (H_3) = H_3\mathcal{M}^+_{m-3}, \tag{48}$$

and Corollary 6.3 proves saturation.

We now determine the restriction kernel. For $P \in \mathcal{L}_m$, direct verification on the two distinguished basis families gives

$$\mathcal{R}_m(\nu_m(P))(z,1) = f(z)^{m-1}\Phi_m(P)\left(z, \frac{g(z)}{f(z)}\right). \tag{49}$$

$$\ell\left(z, \frac{g}{f}\right) = e - Az - \frac{zg}{f} = \frac{r}{f},$$

and the two generator families give, respectively,

$$\mathcal{R}_m(\nu_m(G_{n,i}))(z,1) = z^i f^{\,n-1} r^{\,m-n},$$
$$f^{m-1}\Phi_m(G_{n,i})\left(z, \frac{g}{f}\right) = f^{m-1}\left(\frac{r}{f}\right)^{m-n} z^i = z^i f^{\,n-1} r^{\,m-n},$$

whereas both sides for $G^{(y)}_{k,j}$ equal

$$g^j f^{\,k-j-1} r^{\,m-k}.$$

This verifies (49) term by term.

Because $\gcd(f,g)=1$, the kernel of

$$\mathbb{Q}[z,y] \longrightarrow \mathbb{Q}(z), \qquad y \longmapsto g/f,$$

is the principal ideal $(fy-g)$. Hence the restriction of P vanishes identically if and only if $\Phi_m(P)$ is divisible by $fy-g$. Equation (48) therefore proves the asserted integral kernel. Its quotient has rank $\varrho_m = 4m-2$, equal to $\dim_{\mathbb{Q}} \mathrm{Sym}^{4m-3}(\mathbb{Q}^2)$. The induced restriction is injective over $\mathbb{Q}$, hence an isomorphism over $\mathbb{Q}$. Its integral image is consequently a full-rank sublattice of $\mathrm{Sym}^{4m-3}(\mathbb{Z}^2)$. □

Let

$$K_m = H_3\mathcal{M}^+_{m-3}, \qquad \pi_m = \pi_{K_m}, \qquad Q_m = \pi_m(\mathcal{L}_m) \simeq \mathcal{L}_m/K_m$$

with the orthogonal quotient metric. The lemma shows that a nonzero vector of Q_m represents a polynomial that does not vanish identically on the cubic. At $m=11$, the ranks are

$$n_{11} = 132, \qquad \kappa_{11} = 90, \qquad \varrho_{11} = 42. \tag{50}$$

8.2 The weighted multiplication estimate

We now lower-bound the covolume of the multiplier lattice $H_3\mathcal{M}^+_{m-3}$, because the quotient determinant is the ambient determinant divided by this covolume. The bound retains a power of the height of H_3, which is what makes the direct quotient argument succeed for factors of large height.

Define the weighted height using the graph-normal front embedding:

$$\mathsf{V}(H_3) = \|H_3\|_{X,U,Y}, \tag{51}$$

where the norm is the graph-normal scaled coefficient norm on the eight monomials displayed in Lemma 4.1. We use the fixed canonical normalization from Section 5, so this height is attached to the selected integral factor. Put

$$\alpha_m = \binom{m-1}{3}, \qquad \beta_m = \binom{m}{3}.$$

Lemma 8.3. *There is a constant $c_m > 0$, independent of e, A, X, Y, U and of the normalized H_3 above, such that*

$$\operatorname{covol}(H_3\mathcal{M}^+_{m-3}) \geq c_m\, \mathsf{V}(H_3)^{\kappa_m} e^{3\alpha_m} X^{\alpha_m} U^{3\alpha_m} Y^{\beta_m}. \tag{52}$$

Proof. The estimate separates into a uniform bound for multiplication after scaling and a computation of the remaining weight factors. The scaling reduces the first part to a compact family of multiplication maps. The cofactor basis supplies the second part. Let $\mathscr{H}$ be the real coefficient space spanned by the eight front monomials, let $\mathscr{C}_m$ be the real coefficient space spanned by the graph-normal monomials in the cofactor module (43), and let $\mathscr{P}_m$ be the full graph-normal coefficient space of $\mathcal{L}_m$, of dimension $m(m+1)$. The level-generator shapes show that every product PQ, $P \in \mathscr{H}$, $Q \in \mathscr{C}_m$, lies in $\operatorname{span}_{\mathbb{R}} \mathcal{L}_m$. For the fixed cubic H_3, this is also the inclusion in (48). Thus multiplication lands in the full normal-form coefficient support of $\mathcal{L}_m$.

Scale

$$x = X\xi, \qquad u = U\upsilon, \qquad y = Y\eta, \qquad \beta = (XY)^{-1}.$$

Since $U = XY$, the graph relation becomes

$$\xi\eta = \upsilon - \beta, \qquad 0 < \beta \leq 1.$$

Graph-normal reduction followed by this diagonal scaling is the same as reduction modulo the displayed β-dependent relation. In particular, the multiplication matrices in the fixed bases of $\mathscr{H}, \mathscr{C}_m, \mathscr{P}_m$ have entries polynomial in β, and the scaled coefficient norms become their ordinary Euclidean coefficient norms. Include $\beta = 0$ in the parameter interval. For every $\beta \in [0,1]$, eliminating υ identifies the real quotient ring with $\mathbb{R}[\xi,\eta]$, so it is an integral domain. At the endpoint $\beta = 0$, the normal monomials remain linearly independent:

$$\xi^a\upsilon^b \longmapsto \xi^{a+b}\eta^b, \qquad \eta^j\upsilon^b \longmapsto \xi^b\eta^{j+b} \quad (j \geq 1),$$

and the two exponent regions are disjoint.

The scaled coefficient norm of a graph polynomial is exactly the ordinary coefficient norm after this scaling. On

$$[0,1] \times S(\mathscr{H}) \times S(\mathscr{C}_m),$$

where $S(E)$ denotes the unit sphere of E, the full normal-form coefficient norm of the product is continuous and strictly positive: neither input is zero and the quotient ring is a domain. By the Weierstrass extreme value theorem, this function attains a minimum on the displayed compact set. Its strict positivity gives a constant $a_m > 0$ such that

$$\|PQ\|_{X,U,Y} \geq a_m \|P\|_{X,U,Y} \|Q\|_{X,U,Y}.$$

The constant is effective. After squaring the norm, the minimum is that of a polynomial with rational coefficients over a fixed compact semialgebraic set. Fixed-dimensional real quantifier elimination isolates this positive algebraic minimum and supplies a rational lower bound, making the later threshold constants computable. For fixed nonzero H_3, the resulting linear map

$$M_{H_3} : \mathscr{C}_m \longrightarrow \mathscr{P}_m$$

is injective and satisfies $\sigma_{\min}(M_{H_3}) \geq a_m \mathsf{V}(H_3)$. If the columns of B form a weighted basis of the cofactor lattice, then

$$\operatorname{covol}(M_{H_3}B) = \det(B^{\mathsf{T}} M_{H_3}^{\mathsf{T}} M_{H_3} B)^{1/2} \geq \sigma_{\min}(M_{H_3})^{\kappa_m} \operatorname{covol}(B).$$

Hence multiplication increases its κ_m-dimensional covolume by at least $(a_m \mathsf{V}(H_3))^{\kappa_m}$.

It remains to compute the cofactor covolume. Put $h = m - 3$ and $\alpha_m = \binom{h+2}{3}$. In the same triangular order used in Lemma 6.1, the pure and y-cofactor pivots give

	e	X	U	Y
pure cofactors	$2\alpha_m$	α_m	α_m	0
y-cofactors	α_m	0	$2\alpha_m$	$\binom{h+3}{3}$.

The cofactor module therefore has covolume

$$e^{3\alpha_m} X^{\alpha_m} U^{3\alpha_m} Y^{\beta_m}, \qquad \beta_m = \binom{m}{3}.$$

Multiplying the two bounds and absorbing $a_m^{\kappa_m}$ into the fixed constant c_m proves (52). □

Write

$$X = e^{1/4+\theta}, \qquad \mathsf{V}(H_3) = e^{11/4-\theta+\omega_3}. \tag{53}$$

Using $Y = e^{1/2+O(1/\log e)}$ and $U = e^{3/4+\theta+O(1/\log e)}$, division of (23) by (52) gives

$$\det Q_m \ll e^{m\varrho_m + (6m^2-10m+6)\theta - \kappa_m\omega_3 + O(1/\log e)}. \tag{54}$$

For $m = 11$,

$$\det Q_{11} \ll e^{462+622\theta-90\omega_3+O(1/\log e)}. \tag{55}$$

The leading-exponent condition for a direct quotient vector to satisfy the projected Howgrave–Graham bound at level eleven is

$$\omega_3 > \frac{311}{45}\theta. \tag{56}$$

We choose $m = 11$ because it is the first level at which the direct cubic threshold lies below 7θ, while the m-jet branch still covers $\omega_3 < 7\theta$ with room to absorb the chart and polylogarithmic losses. For general level m, the direct estimate gives the leading threshold

$$\omega_3 > \frac{6m^2 - 10m + 6}{(m-2)(m-1)}\,\theta.$$

This is still $253/36 > 7$ at $m = 10$, but becomes

$$\frac{622}{90} = \frac{311}{45} < 7$$

at $m = 11$. On the jet side, the $m = 11$ inequality

$$20\omega_3 + 286\eta_j < 170\theta$$

covers every $\omega_3 < 7\theta$ after choosing the chart and polylogarithmic losses small relative to θ. Thus the direct construction covers the large-height branch once the margin exceeds the fixed $O(1/\log e)$ loss. We next construct the complementary relation for small heights, and combine the two bounds at the end of the section.

8.3 Integral jets and the exterior estimate

For the small-height branch, we require a restricted polynomial to vanish to a prescribed order at an integer expansion point $z = -j$. A jet is the list of Taylor coefficients that records these conditions. We first normalize the conditions so that they are integer-valued on Q_m, then bound the determinant of their common kernel.

Definition 8.4 (Projective chart and Taylor jet)**.** For a one-variable polynomial $b_0(z) \in \mathbb{Z}[z]_{\le D}$, define the integral Taylor coefficients at $z = -j$ by

$$b_0(s-j) = \sum_{t=0}^{D} \mathrm{jet}_{j,t}(b_0)s^t.$$

Equivalently, homogenize b_0 to

$$B_0(Z, D_0) = D_0^D b_0(Z/D_0) \in \mathrm{Sym}^D(\mathbb{Z}^2).$$

For $j \in \mathbb{Z}$, set $U_0 = Z + jD_0$. The substitution $(Z, D_0) = (U_0 - jD_0, D_0)$ lies in $\mathrm{GL}_2(\mathbb{Z})$, and

$$B_0(U_0 - jD_0, D_0) = \sum_{t=0}^{D} \mathrm{jet}_{j,t}(B_0)U_0^t D_0^{D-t},$$

with the same coefficients: $\mathrm{jet}_{j,t}(B_0) = \mathrm{jet}_{j,t}(b_0)$. We call this integral change of coordinates the *chart at* $z = -j$. The order of vanishing is at least k exactly when $\mathrm{jet}_{j,t}(B_0) = 0$ for $0 \le t < k$, equivalently $U_0^k \mid B_0(U_0 - jD_0, D_0)$.

Choose a positive integer j for which

$$f(-j)g(-j)r(-j) \neq 0,$$

and set

$$\gamma_j = \gcd(|f(-j)|, |g(-j)|), \qquad \eta_j = \log_e \gamma_j. \tag{57}$$

There are at most $3 + 3 + 4 = 10$ excluded integer charts. Use the integral projective change

$$U_0 = Z + jD_0, \qquad Z = U_0 - jD_0.$$

For $P \in \mathcal{L}_m$, define on the quotient Q_m

$$\lambda_{j,t}(\pi_m(P)) = [U_0^t D_0^{4m-3-t}]\, \mathcal{R}_m(P)(U_0 - jD_0, D_0). \tag{58}$$

The value is independent of the chosen integer preimage: by Lemma 8.2, two such preimages differ by $K_m = \ker_{\mathbb{Z}} \mathcal{R}_m$.

The constant coefficients of the transformed forms F, G, R share the divisor γ_j. For $0 \le t < m$, this makes every entry of the t-th Taylor row divisible by γ_j^{m-1-t}. Dividing by this common divisor gives the integer-valued functional needed for the kernel construction.

Lemma 8.5. *For* $0 \le t < m$,

$$\lambda_{j,t}(Q_m) \subseteq \gamma_j^{m-1-t}\mathbb{Z}.$$

Thus

$$\widehat{\lambda}_{j,t} = \gamma_j^{-(m-1-t)}\lambda_{j,t} \tag{59}$$

is an integer-valued functional on Q_m.

Proof. At $U_0 = 0$, the three transformed forms have constant coefficients $f(-j), g(-j), r(-j)$. Moreover,

$$r(-j) = (e + Aj)f(-j) + jg(-j),$$

so γ_j divides all three. Each form in (46) contains $(a + b - 1) + (m - a - b) = m - 1$ factors from F, R. Each form in (47), with its monomial renamed $y^c d^b$, contains

$$c + (b - c - 1) + (m - b) = m - 1$$

factors from G, F, R. To obtain total U_0-degree t, at most t of those factors can contribute a nonconstant term. Powers outside the F, G, R product can only reduce this number. At least $m - 1 - t$ constant terms remain, each divisible by γ_j. Every summand is therefore divisible by γ_j^{m-1-t}. □

It remains to bound the size of these functionals in the dual quotient metric. Their exterior norm measures the volume spanned by the first k Taylor rows; together with the preceding divisibility, it will bound the determinant of the common kernel.

Lemma 8.6. *For fixed m, k with $1 \le k \le m$, the first k unnormalized rows satisfy*

$$\begin{aligned}\|\lambda_{j,0} \wedge \cdots \wedge \lambda_{j,k-1}\| \le C_{m,k}(1 + j)^{C'_{m,k}} \\ \times e^{-k(k+2)/4 + k(m-1)\omega_3 - k(4m-3)\theta},\end{aligned} \tag{60}$$

in the exterior power of the dual quotient metric, with constants independent of the RSA instance and of H_3.

Proof. We rewrite the restriction columns in a fractional linear coordinate and bound their coefficients by degree. A Wronskian identity then bounds the determinants formed by any k columns of the Taylor matrix. Put

$$n = m - 1, \qquad D = 4m - 3, \qquad V = \mathsf{V}(H_3), \qquad L = \frac{U}{X}.$$

After graph reduction there are unique homogeneous forms

$$P_2(x, u) = \sum_{a=0}^{2} \mu_a x^a u^{2-a}, \qquad Q_3(x, u) = \sum_{a=0}^{3} \nu_a x^a u^{3-a}$$

such that

$$H_3 = P_2(x, u) + Q_3(x, u) + c\, y u^3. \tag{61}$$

Graph reduction of $c\, y(Ax + u)^3$ is the expression in (13), whose non-y terms have homogeneous degrees two and three. Consequently the definition of the weighted height is exactly

$$V^2 = \sum_{a=0}^{2} \mu_a^2 X^{2a} U^{2(2-a)} + \sum_{a=0}^{3} \nu_a^2 X^{2a} U^{2(3-a)} + c^2 Y^2 U^6. \tag{62}$$

Set

$$h(z) = e - Az, \qquad \zeta = \frac{z}{h(z)}, \qquad P(\zeta) = P_2(\zeta, 1), \qquad Q(\zeta) = Q_3(\zeta, 1).$$

This ζ is a fractional-linear, or Möbius, coordinate. In the localization at $\bar{f}$,

$$\frac{u}{\bar{f}} = \frac{h}{e}, \qquad \frac{x}{u} = \zeta, \qquad \bar{f}^{-1} = \frac{h - zy}{e}.$$

Dividing (61) by $\bar{f}^3$ and comparing with $fy - g$ gives

$$f = \frac{h^3}{e^3}(c - \zeta P), \qquad g = -\frac{h^3}{e^3}(P + Q), \qquad r = \frac{h^4}{e^3}(c + \zeta Q). \tag{63}$$

After multiplication by e^3, the localized left-hand side is

$$(h - zy)P_2(z,h) + Q_3(z,h) + c\,yh^3 = h^3\big((P+Q) + y(c - \zeta P)\big).$$

The formula for $r = hf - zg$ follows at once.

Define the scaled polynomials

$$\alpha = YU^2(c - \zeta P), \qquad \gamma = U^2(P + Q), \qquad \rho = YU^3(c + \zeta Q). \tag{64}$$

Thus

$$f = \frac{h^3\alpha}{e^3 YU^2}, \qquad g = -\frac{h^3\gamma}{e^3U^2}, \qquad r = \frac{h^4\rho}{e^3YU^3}. \tag{65}$$

Restriction columns. On the parametrized graph,

$$x = \frac{zf}{r}, \qquad u = \frac{hf}{r}, \qquad y = \frac{g}{f}, \qquad Ax + u = \frac{ef}{r}.$$

Verifying first on every generator of $\mathcal{L}_m$, and then using linearity, gives

$$\mathcal{R}_m(P_0)(z,1) = e^{-m}\frac{r(z)^m}{f(z)}P_0\left(\frac{zf}{r}, \frac{hf}{r}, \frac{g}{f}\right) \qquad (P_0 \in \mathcal{L}_m). \tag{66}$$

On the two distinguished generator families, the right-hand side is

$$e^{-m}\frac{r^m}{f}G_{n,i}\left(\frac{zf}{r}, \frac{hf}{r}, \frac{g}{f}\right) = z^i f^{\,n-1} r^{\,m-n},$$
$$e^{-m}\frac{r^m}{f}G^{(y)}_{k,j}\left(\frac{zf}{r}, \frac{hf}{r}, \frac{g}{f}\right) = g^j f^{\,k-j-1} r^{\,m-k},$$

which are exactly the dehomogenizations in (46)–(47).

Restriction support. The triangular proof of Lemma 6.1 shows that the graph-normal coefficient support of $\mathcal{L}_m$ consists exactly of

$$x^a u^b \quad (1 \le a + b \le m), \qquad y^s u^b \quad (1 \le s < b \le m).$$

Use the weighted orthonormal basis of this support. The corresponding restriction columns are

$$\phi_{a,b}(z) = \frac{e^{-m} z^a h^b f^{a+b-1} r^{m-a-b}}{X^a U^b}, \tag{67}$$
$$\phi^{(y)}_{b,s}(z) = \frac{e^{-m} h^b g^s f^{b-s-1} r^{m-b}}{Y^s U^b}. \tag{68}$$

The index ranges are those in the preceding display, so all exponents of f and r are nonnegative.

Put

$$\mathcal{H}_m(z) = \frac{(h(z)/e)^D}{Y^n U^{3m-2}}. \tag{69}$$

Substitution of (63) gives

$$\phi_{a,b} = \mathcal{H}_m \Psi_{a,b}, \qquad \Psi_{a,b}(\zeta) = (L\zeta)^a \alpha(\zeta)^{a+b-1}\rho(\zeta)^{m-a-b}, \tag{70}$$
$$\phi^{(y)}_{b,s} = \mathcal{H}_m \Psi^{(y)}_{b,s}, \qquad \Psi^{(y)}_{b,s}(\zeta) = (-\gamma(\zeta))^s \alpha(\zeta)^{b-s-1}\rho(\zeta)^{m-b}. \tag{71}$$

Every Ψ contains exactly $n = m - 1$ factors from α, γ, ρ, besides the displayed factor $(L\zeta)^a$.

Coefficient bounds by degree. The next bound controls every restriction column and hence every minor of the Taylor matrix. Equation (62) gives

$$|\mu_a| \le VU^{-2}L^a, \qquad |\nu_a| \le VU^{-3}L^a, \qquad |c| \le \frac{V}{YU^3}.$$

Since $L = U/X = Y$, the definitions in (64) imply, coefficient by coefficient,

$$|[\zeta^\ell]\alpha| + |[\zeta^\ell]\gamma| + |[\zeta^\ell]\rho| \le C_m V L^\ell. \tag{72}$$

For instance, for $\ell \ge 1$,

$$YU^2|\mu_{\ell-1}| \le VYL^{\ell-1} \le VL^\ell, \qquad YU^3|\nu_{\ell-1}| \le VYL^{\ell-1} \le VL^\ell.$$

The constant terms and the coefficients of γ follow directly from the same three bounds. Products of these fixed-degree polynomials therefore satisfy

$$|[\zeta^\ell]\Psi| \le C_m V^n L^\ell \tag{73}$$

for every column in either family. More explicitly, each coefficient is a sum of $O_m(1)$ products indexed by $\ell_1 + \cdots + \ell_n = \ell$. The factor bounds in (72) multiply to $V^n L^{\ell_1+\cdots+\ell_n} = V^n L^\ell$. For the pure family, the extra monomial $(L\zeta)^a$ merely replaces ℓ by $\ell - a$ and contributes L^a, leaving the same total power L^ℓ. Here $V \ge |c|YU^3 \ge 1$.

At the chart point

$$\zeta_j = -\frac{j}{e + Aj}, \qquad L|\zeta_j| \le \frac{L}{A} < 1$$

for all sufficiently large RSA instances. Since all degrees are bounded in terms of m, differentiating (73) gives

$$|\Psi^{(\ell)}(\zeta_j)| \le C_m V^n L^\ell \qquad (0 \le \ell < k). \tag{74}$$

Wronskian bound. For a variable s, define

$$W_s(\psi_1, \dots, \psi_k) = \det\big(\partial_s^{i-1}\psi_j\big)_{1\le i,j\le k}.$$

Choose arbitrary k columns, in any mixture of the two families. The common-factor and change-of-variable Wronskian formulas are exact:

$$W_z(\mathcal{H}_m\Psi_1(\zeta), \dots, \mathcal{H}_m\Psi_k(\zeta)) = \mathcal{H}_m^k(\zeta')^{\binom{k}{2}} W_\zeta(\Psi_1, \dots, \Psi_k), \qquad \zeta' = \frac{e}{h^2}. \tag{75}$$

They follow from lower-triangular transformations of the derivative rows. The two diagonals are

$$(\mathcal{H}_m, \dots, \mathcal{H}_m) \quad \text{and} \quad (1, \zeta', \dots, (\zeta')^{k-1}),$$

respectively. For the selected columns $\phi_1, \dots, \phi_k$, the corresponding Taylor minor is exactly

$$\det\left(\frac{\phi_q^{(p)}(-j)}{p!}\right)_{\substack{0\le p\le k-1\\ 1\le q\le k}} = \frac{W_z(\phi_1, \dots, \phi_k)(-j)}{\prod_{p=0}^{k-1} p!}.$$

Thus conversion from derivatives to Taylor coefficients contributes only the displayed fixed factorial. Hadamard's inequality and (74) therefore bound every mixed Taylor minor by

$$C_{m,k}|\mathcal{H}_m(-j)|^k V^{nk}(|\zeta'(-j)|L)^{\binom{k}{2}}. \tag{76}$$

The remaining scale calculations are

$$|\mathcal{H}_m(-j)|V^n \le C_m(1+j)^D e^{-3/4+n\omega_3-D\theta}. \tag{77}$$

$$|\zeta'(-j)|L = \frac{eU}{X(e+Aj)^2} \le \frac{U}{eX} \le Ce^{-1/2}. \tag{78}$$

$A/e = \Theta(1)$, $Y = e^{1/2+O(1/\log e)}$, and $U = e^{3/4+\theta+O(1/\log e)}$. In (77) the constant and θ-exponents are

$$n\frac{11}{4} - \frac{n}{2} - (3m-2)\frac{3}{4} = -\frac{3}{4}, \qquad -n - (3m-2) = -(4m-3).$$

Combining (76)–(78) gives

$$|\mathrm{minor}| \le C_{m,k}(1+j)^{Dk} e^{-k(k+2)/4 + kn\omega_3 - kD\theta},$$

because

$$-\frac{3k}{4} - \frac{1}{2}\binom{k}{2} = -\frac{k(k+2)}{4}.$$

The support has the fixed $m(m+1)$ columns listed above. Cauchy–Binet turns the uniform mixed-minor bound into the same bound, up to a constant depending only on m, k, for the ambient exterior row norm. To identify the metric precisely, put

$$E = \mathrm{span}_{\mathbb{R}}\, \mathcal{L}_m, \qquad E_K = \mathrm{span}_{\mathbb{R}}\, K_m.$$

Each restriction row is a functional on E that annihilates E_K. Its Riesz vector therefore belongs to $E_K^{\perp}$, while orthogonal projection identifies the quotient E/E_K isometrically with $E_K^{\perp}$. Under this identification the Riesz map preserves the row norm and every exterior norm. Hence the ambient exterior norm just bounded is exactly the dual quotient exterior norm in (60). This proves the lemma. □

The projective shear contributes only the factor $(1+j)^{C'_{m,k}}$. The Wronskian calculation bounds the rows using polynomial expressions in f, g, r, so the estimate is uniform even when $|r(-j)|$ is small. We now convert the exterior norm bound into a determinant bound.

Lemma 8.7. *Let Λ be a rank-r Euclidean lattice and let $\ell_0, \dots, \ell_{k-1} \in \Lambda^*$ be linearly independent integer-valued functionals. Put $K = \{v \in \Lambda : \ell_t(v) = 0 \text{ for every } t\}$. Then K is saturated, has rank $r-k$, and*

$$\det K \le \det \Lambda\, \|\ell_0 \wedge \cdots \wedge \ell_{k-1}\|. \tag{79}$$

Proof. The homomorphism $\ell : \Lambda \to \mathbb{Z}^k$ identifies Λ/K with the torsion-free image lattice $\ell(\Lambda)$, so K is saturated. Choose a basis of the image lattice and lift it to Λ. The Gram determinant formula for this exact sequence gives

$$\det K = \frac{\det \Lambda\, \|\ell_0 \wedge \cdots \wedge \ell_{k-1}\|}{[\mathbb{Z}^k : \ell(\Lambda)]}.$$

The index in the denominator is a positive integer, proving the bound. □

Apply this lemma to

$$\mathcal{K}_{m,j,k} = \bigcap_{t=0}^{k-1} \ker \widehat{\lambda}_{j,t} \subseteq Q_m.$$

Lemma 8.2 identifies $Q_m \otimes \mathbb{Q}$ with the full binary-form space, so the first k coefficient functionals are rationally independent and $\mathrm{rank}\, \mathcal{K}_{m,j,k} = \varrho_m - k$. Lemma 8.7, Lemma 8.5, and the exterior estimate give

$$\det \mathcal{K}_{m,j,k} \le \det Q_m\, \gamma_j^{-k(m-1)+\binom{k}{2}}\, \|\lambda_{j,0} \wedge \cdots \wedge \lambda_{j,k-1}\|.$$

For $m = k = 11$, combining this inequality with (55) yields

$$\mathrm{rank}\, \mathcal{K}_{11,j,11} = 31, \qquad \det \mathcal{K}_{11,j,11} \ll (1+j)^{C} e^{1705/4 + 171\theta + 20\omega_3 - 55\eta_j}. \tag{80}$$

The exponent identities are

$$462 - \frac{143}{4} = \frac{1705}{4}, \quad 622 - 451 = 171, \quad -90 + 110 = 20, \quad -110 + 55 = -55.$$

Thus the eleven Taylor conditions leave a rank-31 lattice with the determinant bound needed to control evaluation at the target.

8.4 Integer identity and gcd control

The jet conditions will produce the second relation once we show that its formal lift evaluates to zero at the RSA point. We isolate that task in an integer w: the upper bound from the jet kernel will be compared with a lower bound that holds whenever w is nonzero.

Take a shortest nonzero vector $\mathbf{v} \in \mathcal{K}_{11,j,11}$. For the proof, choose any $P \in \mathcal{L}_{11}$ with $\pi_{11}(P) = \mathbf{v}$, and set

$$w = \nu_{11}(P)(x_0, d, y_0) = \frac{P(x_0, u_0, y_0)}{e^{11}} \in \mathbb{Z}.$$

Write

$$F_j(U_0, D_0) = F(U_0 - jD_0, D_0), \qquad G_j(U_0, D_0) = G(U_0 - jD_0, D_0).$$

At the target, (41) gives

$$F(x_0, d) = d^3 f(z_0) = d^4 r(z_0) = R(x_0, d).$$

The definition of restriction therefore gives

$$\mathcal{R}_{11}(P)(x_0, d) = F(x_0, d)^{10} w.$$

The eleven jet equations make the integral binary form $\mathcal{R}_{11}(P)(U_0 - jD_0, D_0)$ divisible by U_0^{11}. Division by this monic factor is integral, so there is $L_j \in \mathbb{Z}[U_0, D_0]$ with

$$F_j(x_0 + jd, d)^{10} w = (x_0 + jd)^{11} L_j(x_0 + jd, d). \tag{81}$$

Lemma 8.8. *For the chart and target defined above,*

$$\gcd(x_0 + jd, F_j(x_0 + jd, d)) \mid \gamma_j. \tag{82}$$

Consequently, if $w \neq 0$, then

$$|w| \geq \left(\frac{|x_0 + jd|}{\gamma_j} \right)^{11}. \tag{83}$$

Proof. Put $v = x_0 + jd$. Equation (2) gives $\gcd(v, d) = 1$. Modulo v,

$$F_j(v, d) \equiv d^3 f(-j), \qquad G_j(v, d) \equiv d^3 g(-j).$$

At the target, $G_j(v, d) = y_0 F_j(v, d)$. Hence every prime power dividing both v and $F_j(v, d)$ divides both $f(-j)$ and $g(-j)$, because d is invertible modulo that prime power. This proves (82).

Here $F_j(v, d) = F(x_0, d) = d^3 f(z_0) \neq 0$, by the choice of the cubic chart at the target. For a rational prime ϖ, let $a_\varpi = v_\varpi(v)$, $b_\varpi = v_\varpi(F_j(v, d))$, and $g_\varpi = v_\varpi(\gamma_j)$. The integer identity gives

$$v_\varpi(w) \geq 11a_\varpi - 10b_\varpi,$$

while (82) gives $\min\{a_\varpi, b_\varpi\} \leq g_\varpi$. If $b_\varpi \geq a_\varpi$, then $a_\varpi \leq g_\varpi$, so the desired local lower bound is trivial. If $b_\varpi < a_\varpi$, then $b_\varpi \leq g_\varpi$ and

$$v_\varpi(w) \geq 11a_\varpi - 10b_\varpi = 11(a_\varpi - b_\varpi) + b_\varpi \geq 11(a_\varpi - b_\varpi) \geq 11(a_\varpi - g_\varpi).$$

Thus $v_\varpi(w) \geq 11(a_\varpi - g_\varpi)_+$ in both cases. Multiplying over all primes,

$$|w| \geq \prod_{\varpi} \varpi^{11(v_\varpi(v)-v_\varpi(\gamma_j))_+} \geq \left(\frac{|v|}{\gamma_j}\right)^{11},$$

which proves (83). □

For positive j, $|x_0+jd| \geq d \geq X/2$. Minkowski in the rank-31 jet kernel, projected evaluation, and (80) give

$$|w| \ll e^{-11}(\det \mathcal{K}_{11,j,11})^{1/31}.$$

Comparison with (83) forces $w = 0$, up to the explicit polylogarithmic chart factor, when

$$20\omega_3 + 286\eta_j < 170\theta. \tag{84}$$

This is the leading-exponent condition. Fixed constants and the chart factor contribute the lower-order terms recorded below.

8.5 Resultant averaging and the high–low split

The low-height jet branch needs a chart for which γ_j is only polylogarithmic. We find one by bounding the coefficient and resultant heights, controlling each prime valuation, and averaging over $O(\log e)$ charts. Irreducibility gives $\gcd(f, g) = 1$, while canonical primitivity gives joint coefficient content one.

Lemma 8.9. *The canonically normalized fixed-degree polynomials f, g, r have coefficients of magnitude $e^{O(1)}$. In particular, the nonzero integer*

$$R_{f,g} = \operatorname{Res}(f, g)$$

satisfies $1 \leq |R_{f,g}| \leq e^{C_{\mathrm{R}}}$ for an effective absolute constant C_{R}.

Proof. The front lattice contains e^3x^2, so its shortest nonzero vector P_3 satisfies $\|P_3\|_{X,U,Y} \leq e^3X^2 = e^{O(1)}$, since $X \leq 2N$ in the ranges under consideration and $e = \Theta(N)$. All column weights are at least one, so the graph-normal coefficients of P_3 have height $e^{O(1)}$. Let T be the unweighted eight-by-eight front matrix obtained from the matrix in Lemma 4.1 by deleting the column weights. Then $\det T = e^{12}$, all entries of T are $e^{O(1)}$, and

$$T^{-1} = e^{-12}\operatorname{adj}(T)$$

also has entries $e^{O(1)}$, since the size is fixed. Thus the graph-normal coefficient height and the front-row coordinate height differ by at most an $e^{O(1)}$ factor. The fixed-size canonical-pair map and its inverse likewise have entries $e^{O(1)}$, because $A = e^{O(1)}$. Hence the coefficients entering the canonical factorization all have height $e^{O(1)}$.

We first control the height of integral factors. If a fixed-degree $P \in \mathbb{Z}[z]$ has height H, every complex root has modulus at most $1 + H$ by the Cauchy root bound. In a primitive Gauss factorization, the leading coefficient of an integral factor divides the leading coefficient of P. Expanding that factor as a product of at most $\deg P$ linear factors therefore bounds its coefficients by $2^{O(1)}H(1 + H)^{O(1)}$. Apply this separately to each nonzero member of the original canonical pair, its primitive gcd, and the corresponding integral quotients. Hence the normalized irreducible factor, and its canonical pair $(f, -g)$, still have height $e^{O(1)}$. Equation (40) gives the same bound for r.

Finally $\deg f, \deg g \leq 3$. Hadamard's inequality on the Sylvester matrix gives, for $H_0 = \max\{\|f\|_\infty, \|g\|_\infty, 1\}$,

$$|R_{f,g}| \leq \|f\|_2^{\deg g}\|g\|_2^{\deg f} \leq (2H_0)^6 = e^{O(1)}.$$

Coprimality makes $R_{f,g}$ a nonzero integer, and every constant in the displayed fixed-degree estimates is effective. □

Valuations. To average the common factors of $f(-j)$ and $g(-j)$, we estimate their prime-power divisibility one prime at a time. For each rational prime ϖ, fix an extension of the additive valuation v_ϖ to $\overline{\mathbb{Q}}_\varpi$, normalized by $v_\varpi(\varpi) = 1$, and put $v_\varpi(0) = +\infty$. For a nonzero polynomial $H(z) = \sum_i h_i z^i$, its *Gauss valuation* is

$$v_{\mathrm{G}}(H) = \min_i v_\varpi(h_i).$$

The Gauss lemma gives $v_{\mathrm{G}}(H_1H_2) = v_{\mathrm{G}}(H_1) + v_{\mathrm{G}}(H_2)$: after scaling both factors to Gauss valuation zero, their nonzero reductions multiply nontrivially in the residue-field polynomial ring. Consequently, if

$$H(z) = a\prod_\nu (z - \alpha_\nu),$$

with roots counted with multiplicity, then

$$v_{\mathrm{G}}(H) = v_\varpi(a) + \sum_\nu \min\{0, v_\varpi(\alpha_\nu)\}. \tag{85}$$

Lemma 8.10. *Fix $D \geq 1$. Let $F_0, G_0 \in \mathbb{Z}[z]$ be nonzero polynomials of degree at most D, at least one of positive degree. Assume that they are coprime over $\mathbb{Q}[z]$ and that the gcd of all their coefficients is one. Put*

$$\mathfrak{R}_0 = \mathrm{Res}(F_0, G_0) \neq 0, \qquad \Gamma_j = \gcd(|F_0(-j)|, |G_0(-j)|).$$

There is an effective constant C_D, depending only on D, such that for every integer $J \geq 2$,

$$\prod_{j=1}^{J} \Gamma_j \leq J^{C_D J}|\mathfrak{R}_0|^{2D}. \tag{86}$$

Proof. The integral Sylvester-adjugate identity gives $S, T \in \mathbb{Z}[z]$ such that

$$\mathfrak{R}_0 = SF_0 + TG_0.$$

Thus, for every rational prime ϖ, if $s_\varpi = v_\varpi(\mathfrak{R}_0)$, then

$$v_\varpi(\Gamma_j) \leq s_\varpi. \tag{87}$$

Fix $\varpi \mid \mathfrak{R}_0$. Joint primitivity implies that one of F_0, G_0, denoted H_ϖ, is ϖ-primitive. Hence

$$v_\varpi(\Gamma_j) \leq \min\{s_\varpi, v_\varpi(H_\varpi(-j))\}. \tag{88}$$

Factor over $\overline{\mathbb{Q}}_\varpi$:

$$H_\varpi(z) = a\prod_{\nu=1}^{h}(z - \alpha_\nu), \qquad h \leq D,$$

with roots counted with multiplicity and $v_\varpi(\varpi) = 1$. The Gauss valuation of a primitive polynomial is zero, so

$$v_\varpi(a) + \sum_{\nu=1}^{h} \min\{0, v_\varpi(\alpha_\nu)\} = 0. \tag{89}$$

For an integer n, a root with negative valuation satisfies $v_\varpi(n - \alpha_\nu) = v_\varpi(\alpha_\nu)$. Its contribution therefore cancels the corresponding leading-coefficient contribution in (89). Using $\min(B, \sum_\nu b_\nu) \leq \sum_\nu \min(B, b_\nu)$ for nonnegative b_ν, we obtain

$$\min\{s_\varpi, v_\varpi(H_\varpi(n))\} \leq \sum_{\substack{1\leq\nu\leq h\\ v_\varpi(\alpha_\nu)\geq 0}} \min\{s_\varpi, v_\varpi(n - \alpha_\nu)\}.$$

Fix a ϖ-adically integral root α, so that $v_\varpi(\alpha) \geq 0$. If two integers j_1, j_2 satisfy $v_\varpi(-j_i - \alpha) \geq t > 0$, then $v_\varpi(j_1 - j_2) \geq t$. Since the valuation of a rational integer is integral, they are congruent modulo $\varpi^{\lceil t \rceil}$. Hence

$$\#\{1 \leq j \leq J : v_\varpi(-j-\alpha) \geq t\} \leq \frac{J}{\varpi^{\lceil t \rceil}} + 1.$$

Integrating this counting bound gives

$$\begin{aligned}\sum_{j=1}^{J} \min\{s_\varpi, v_\varpi(-j-\alpha)\} &= \int_0^{s_\varpi} \#\{1 \leq j \leq J : v_\varpi(-j-\alpha) \geq t\}\, dt \\ &\leq \frac{J}{\varpi - 1} + s_\varpi.\end{aligned}$$

Summing over the at most D roots, including multiplicities, yields

$$\sum_{j=1}^{J} v_\varpi(\Gamma_j) \leq D\left(\frac{J}{\varpi - 1} + s_\varpi\right). \tag{90}$$

For $\varpi > J$, $J/(\varpi - 1) \leq 1 \leq s_\varpi$. For $\varpi \leq J$, keep the first term in (90). Thus

$$\prod_{j=1}^{J} \Gamma_j \leq |\mathfrak{R}_0|^{2D} \left(\prod_{\varpi \leq J} \varpi^{1/(\varpi-1)}\right)^{DJ}.$$

The elementary Chebyshev estimate $\vartheta(T) = \sum_{\varpi \leq T} \log \varpi \ll T$ follows because the product of the primes $n < \varpi \leq 2n$ divides $\binom{2n}{n} < 4^n$, followed by dyadic summation. Partial summation then gives

$$\sum_{\varpi \leq J} \frac{\log \varpi}{\varpi - 1} \leq 2\left(\frac{\vartheta(J)}{J} + \int_2^J \frac{\vartheta(t)}{t^2}\, dt\right) \ll 1 + \log J.$$

The prime product is therefore $J^{O(1)}$, proving (86). □

The pair $(f, -g)$ is the canonical pair of the canonically primitive polynomial H_3, so f, g have joint coefficient content one. Apply Lemma 8.10 with $D = 3$. There are at most $\deg f + \deg g + \deg r \leq 10$ bad positive charts. For $J \geq 20$, let

$$\mathscr{J}_J = \{1 \leq j \leq J : f(-j)g(-j)r(-j) \neq 0\}.$$

Then $|\mathscr{J}_J| \geq J/2$, and deleting factors cannot increase their product. Consequently

$$\begin{aligned}\min_{j \in \mathscr{J}_J} \gamma_j &\leq \left(\prod_{j=1}^{J} \gcd(|f(-j)|, |g(-j)|)\right)^{1/(J-10)} \\ &\leq J^{C_0} |R_{f,g}|^{C_1/J}\end{aligned} \tag{91}$$

for effective absolute constants C_0, C_1.

Take $J = \max\{20, \lceil \log e \rceil\}$. Lemmas 8.9 and 8.10 give a deterministically computable good chart with

$$\gamma_j = (\log e)^{O(1)}, \qquad \eta_j = O\left(\frac{\log\log e}{\log e}\right). \tag{92}$$

All $O(\log e)$ evaluations have polynomial bit length, and fixed-degree evaluation, Euclidean gcd, and selection of the smallest value are deterministic polynomial-time operations.

The following proposition collects the two constructions, including their lower-order losses.

Proposition 8.11 (Recovery on a cubic component)**.** *Retain the RSA size bounds and notation of this section. Let H_3 be a canonically primitive irreducible factor of the shortest front relation P_3, of exact canonical degree three and of the form* (39)*. Assume $H_3(x_0, u_0, y_0) = 0$ and $X/2 \le d \le X$. Define θ, ω_3 by* (53)*, assume $\theta > 0$, and put $J = \max\{20, \lceil \log e \rceil\}$.*

There are effective positive constants $C_{\mathrm{dir}}, C_{\mathrm{chart}}, C_{\mathrm{abs}}$ such that, for all e above an effective threshold, either of the following conditions ensures recovery:

1. *$\omega_3 \ge 7\theta$ and $8\theta > C_{\mathrm{dir}}/\log e$;*
2. *$\omega_3 < 7\theta$ and some $j \in \mathscr{J}_J$ satisfies*

$$20\omega_3 + 286\eta_j + C_{\mathrm{chart}} \frac{\log\log e}{\log e} + \frac{C_{\mathrm{abs}}}{\log e} < 170\theta. \tag{93}$$

In the first case use the rank-42 quotient Q_{11}; in the second use the rank-31 kernel $\mathcal{K}_{11,j,11}$. Each construction computes, in deterministic polynomial time in $\log N$, a relation $P_3' \in \mathcal{G}_{\mathbb{Z}}$ satisfying

$$P_3'(x_0, u_0, y_0) = 0, \qquad P_3' \notin (H_3).$$

Elimination with H_3 then produces a finite candidate set containing the RSA root.

In particular, there is an effective constant C_* such that one of the two cases applies whenever

$$\theta \ge C_* \frac{\log\log e}{\log e}.$$

All constants depend only on the fixed lattice levels and RSA size bounds.

Proof. If $\omega_3 \ge 7\theta$, equation (55) gives

$$\det Q_{11} \ll e^{462 - 8\theta + O(1/\log e)},$$

so the rank-42 direct branch has a saving of 8θ in its determinant exponent. A sufficiently large effective C_{dir} absorbs the fixed constants in Minkowski's bound and projected evaluation, proving the first case.

For the rank-31 jet kernel, (80) and Lemma 8.8 give the second case. The constants in (93) account for $(1 + j)^C$, Minkowski's bound, evaluation, and the fixed RSA size bounds. Since $j \le J$, their contribution has the stated order.

To verify the final assertion, choose the chart supplied by (92). For sufficiently large C_*, its gcd bound gives $\eta_j < \theta/20$. If $\omega_3 < 7\theta$ and $\eta_j < \theta/20$, then

$$20\omega_3 + 286\eta_j < 140\theta + \frac{286}{20}\theta < 155\theta < 170\theta,$$

so more than 15θ remains to absorb the two lower-order losses. Increasing C_* if necessary also ensures the direct condition.

In either branch, the selected nonzero rational quotient vector vanishes at the RSA root and lies outside (H_3). Clearing denominators gives an integer relation with the same properties. Since H_3 is irreducible, the pair is coprime and fixed-degree zero-dimensional elimination recovers finitely many candidates. The lattice ranks and polynomial degrees are fixed, and Lemma 8.9 bounds the coefficient bit lengths, so these operations have polynomial bit complexity. □

The constants in this proposition are fixed before the transition parameter K in the next section is chosen. Taking that parameter sufficiently large will place every remaining dyadic range above the stated lower bound on θ.

9 Algorithmic completion

We now combine the preceding constructions into a deterministic algorithm. It first searches the range near Wiener's bound using a two-dimensional lattice, then explores the larger dyadic ranges. In each range, it tests the candidates by reconstructing and verifying the factors of N. The unknown value of d is used only in the correctness proof.

9.1 Two-dimensional transition lattice and dyadic ranges

Fix an effectively computable, sufficiently large integer $K \in \mathbb{Z}_{>0}$, and put

$$\ell_N = \lceil \log_2 N \rceil, \qquad D_{\mathrm{tr}} = \lfloor N^{1/4} \rfloor \, \ell_N^K.$$

The algorithm first sets $X = D_{\mathrm{tr}}$, $Y = 3\lceil \sqrt{N} \rceil$, and $U = XY$, and constructs the two-dimensional integer lattice

$$\Lambda_{\mathrm{tr}} = \langle (eX, 0), (AX, U) \rangle_{\mathbb{Z}} \subset \mathbb{R}^2.$$

Write a lattice vector as (aX, bU). Then there is an integer r with

$$a = er + Ab,$$

and the vector corresponds to the linear polynomial

$$P_{a,b}(x, u) = ax + bu.$$

At the RSA point, using $Ax_0 + u_0 = ed$,

$$P_{a,b}(x_0, u_0) = e(rx_0 + bd). \tag{94}$$

Compute an exact shortest nonzero vector (aX, bU) of Λ_{tr}. To see why this step covers $d \le D_{\mathrm{tr}}$, assume this bound for the moment. The choice $r = -d$, $b = x_0$ gives the comparison vector $(-u_0 X, x_0 U) \in \Lambda_{\mathrm{tr}}$. Since $x_0 < d \le X$ and $|u_0| \le U$, shortestness implies

$$\|(aX, bU)\|_2 \le \sqrt{2}\, XU.$$

Consequently

$$|P_{a,b}(x_0, u_0)| \le |a|X + |b|U \le 2\sqrt{2}\, XU,$$

and (94) gives

$$|rx_0 + bd| \le 2\sqrt{2}\, \frac{XU}{e} \le \ell_N^{O_K(1)}.$$

Lemma 9.1. *Take $X = D_{\mathrm{tr}}$, $Y = 3\lceil \sqrt{N} \rceil$, and $U = XY$ as above. Let $v = (aX, bU)$ be a shortest nonzero vector of Λ_{tr}, and write $a = er + Ab$. Define*

$$H_{\mathrm{tr}} = \left\lceil 2\sqrt{2}\, \frac{XU}{e} \right\rceil.$$

All integer pairs (x, d) satisfying

$$\begin{aligned} &1 \le x < d \le X, \quad \gcd(x, d) = 1, \\ &|ed - Ax| \le U, \quad |rx + bd| \le H_{\mathrm{tr}} \end{aligned}$$

can be enumerated deterministically in $(\log N)^{O_K(1)}$ time.

Proof. First $\gcd(r, b) = 1$. Otherwise, if $g = \gcd(r, b) > 1$, then $g \mid a$, and $(aX/g, bU/g)$ would be a shorter nonzero vector of Λ_{tr}.

For a candidate pair put $u = ed - Ax$ and

$$w(x, d) = (-uX, xU) = -d(eX, 0) + x(AX, U) \in \Lambda_{\mathrm{tr}}.$$

The bounds on x and u give

$$\|w(x, d)\|_2 \le \sqrt{2}\, XU =: R.$$

Moreover

$$\begin{aligned} \det(v, w(x, d)) &= XU(ax + bu) \\ &= XU\big((er + Ab)x + b(ed - Ax)\big) \\ &= eXU(rx + bd). \end{aligned}$$

Since $\det \Lambda_{\mathrm{tr}} = eXU$, the integer

$$h = rx + bd$$

is the determinant index of the pair $(v, w(x, d))$.

Fix $h \neq 0$. The area bound gives

$$\|v\|_2 \|w(x, d)\|_2 \ge |h| eXU,$$

so

$$\|v\|_2 \ge \frac{|h|e}{\sqrt{2}}.$$

All integer solutions of $rx + bd = h$ differ by

$$(x, d) \mapsto (x + tb, d - tr), \qquad t \in \mathbb{Z},$$

and the corresponding lattice vectors satisfy

$$w(x + tb, d - tr) = w(x, d) + tv.$$

Hence, inside the ball $\|w\|_2 \le R$, the number of candidates for this fixed nonzero h is at most

$$1 + \frac{2R}{\|v\|_2} \le 1 + \frac{4XU}{|h|e}.$$

Summing over $1 \le |h| \le H_{\mathrm{tr}}$ gives

$$\sum_{1 \le |h| \le H_{\mathrm{tr}}} \left(1 + O\left(\frac{XU}{|h|e}\right)\right) = O(H_{\mathrm{tr}} \log H_{\mathrm{tr}}) = (\log N)^{O_K(1)}.$$

For $h = 0$, the solutions have the form $(x, d) = t(b, -r)$. Since $\gcd(r, b) = 1$ and $\gcd(x, d) = 1$, one has $t = \pm 1$, and the positivity conditions leave at most one candidate.

For $h = 0$, test the at most one primitive positive candidate identified above. For each nonzero enumerated h, compute one solution of $rx + bd = h$ by extended Euclid, write all solutions as

$$(x, d) = (x_*, d_*) + t(b, -r),$$

intersect the resulting arithmetic progression with

$$1 \le x < d \le X, \qquad |ed - Ax| \le U,$$

and verify the resulting RSA candidates. Since $H_{\mathrm{tr}} = (\log N)^{O_K(1)}$, the count above proves that the total number of verified candidates is polylogarithmic. □

If $d \le D_{\mathrm{tr}}$, the target pair satisfies all the conditions of Lemma 9.1, including $|rx_0 + bd| \le H_{\mathrm{tr}}$. The procedure therefore lists that pair, and RSA verification identifies it.

If no candidate passes verification, the algorithm sets $X_t = 2^t D_{\mathrm{tr}}$ for $1 \le t \le T$, where T is the least nonnegative integer for which $2^T D_{\mathrm{tr}} \ge N$. It explores the ranges

$$X_t/2 < d \le X_t.$$

There are $O(\log N)$ such ranges. If $d > D_{\mathrm{tr}}$, the least index t with $X_t \ge d$ satisfies $d \le X_t < 2d$; in this case $T \ge 1$ and $X_T < 2N$. This is the range used in the correctness proof. Write $X = X_t$. Then

$$\theta = \log_e X - \frac{1}{4} \ge K \frac{\log\log N}{\log e} - O(1/\log e). \tag{95}$$

On the other hand, $d \le N^{11/42-\varepsilon}$, $X < 2d$, and $e = \Theta(N)$ imply

$$\theta \le \frac{1}{84} - \frac{\varepsilon}{2} \tag{96}$$

for all sufficiently large N. Thus the front lattice has a fixed power saving, while a sufficiently large fixed K makes (92) smaller than $\theta/20$ and absorbs the explicit factor $(1+j)^C$ in the proved jet bound.

9.2 Branching, complexity, and verification

The complete procedure has input (N, e) and the fixed parameter ε. It returns verified factors p, q and the least positive private exponent, or reports failure if no candidate passes verification. Under the hypotheses of Theorem 1.1, a successful branch is guaranteed. The constants K and N_0 below are fixed by the proof.

1. For $N < N_0$, factor N by trial division and compute the private exponent. For larger inputs, run the transition enumeration of Lemma 9.1 and test its candidates.
2. If no candidate passes, process each dyadic range defined above. Set $X = X_t$, build the eight-row lattice, compute an exact shortest vector, and denote its polynomial by P_3.
3. Compute the canonical pair and its normalized factorization. For every factor involving only z, recover the candidate pair (x, d). For every factor fixing y, recover the candidate factors of N.
4. For each remaining H_1 or H_2, form the saturated quotient from Lemma 7.1 or Lemma 7.2. Compute a shortest nonzero quotient vector, clear denominators, and eliminate with H_1 or H_2.
5. For each H_3, run the direct quotient construction and the integral-jet construction for every $j \in \mathscr{J}_J$, where $J = \max\{20, \lceil \log e \rceil\}$. Clear the denominators of each resulting nonzero vector and eliminate with H_3.
6. Test every candidate by the verification procedure below. Return the factors and private exponent at the first success; if all ranges have been exhausted, report failure.

Recovering candidates. An eliminated solution (x, y) determines

$$u = 1 + xy, \qquad d = \frac{Ax + u}{e}.$$

Keep it when the latter quotient is a positive integer in the current dyadic range. A branch defined by a factor in z only instead recovers the reduced pair (x, d) directly. A fixed-y branch factors N and then computes the least positive inverse of e mod $\varphi(N)$.

When a coordinate resultant vanishes, the algorithm tries the other coordinate and a fixed list of rational linear changes, or equivalently computes a lexicographic Gröbner basis. It back-substitutes every rational univariate root and checks the resulting candidates in both original polynomials, discarding any extraneous resultant roots.

Bit complexity. The lattice of rank 132 occurs as an ambient space for saturation, quotient, restriction, and kernel computations. The largest exact SVP instance has rank 42, and the final jet kernel has rank 31. Exact SVP for a fixed-dimensional integer lattice or rational Gram form, HNF/SNF, rational projection, fixed-degree factorization, and fixed-degree resultant elimination have polynomial bit complexity.

The ambient lattice bases, multiplier bases, and jet functionals have polynomial bit length. Since all ranks and degrees are fixed, determinants of the corresponding Gram and projection matrices also have polynomial bit length. Thus exact orthogonal projection produces numerators and denominators of polynomial bit length, and clearing a common denominator gives an equivalent integral quadratic form of polynomial bit size. The same observation applies to the normalized jet kernels and to integer lifts of quotient vectors. The number of dyadic ranges is $O(\log N)$, the number of charts is $O(\log e)$, and the transition branch enumerates only polylogarithmically many values of h. All constants in the norm and height estimates are effective. The proof inequalities therefore compute an explicit threshold N_0. Inputs $N < N_0$ are handled by deterministic trial division (or a precomputed finite table), at a constant cost depending only on the fixed theorem parameters.

Final RSA verification. For every candidate pair (x, d), require $x, d > 0$, membership in the current dyadic range (or $d \le D_{\mathrm{tr}}$ in the transition branch), and $\gcd(x, d) = 1$. For each surviving pair, compute

$$\varphi' = \frac{ed-1}{x}, \qquad s' = N + 1 - \varphi', \qquad \Delta = (s')^2 - 4N.$$

Retain it when φ' is integral, $\Delta \ge 0$ is a square, and $s' \pm \sqrt{\Delta}$ are positive even integers. Set

$$(p', q') = \left(\frac{s' - \sqrt{\Delta}}{2}, \frac{s' + \sqrt{\Delta}}{2} \right),$$

Then check $1 < p' < q' < 2p'$, $p'q' = N$, and $ed \equiv 1 \pmod{(p'-1)(q'-1)}$. Output the least positive inverse of $e \bmod (p'-1)(q'-1)$. This inverse is the original least positive private exponent specified in Theorem 1.1.

Proof of Theorem 1.1. The transition step covers $d \le D_{\mathrm{tr}}$. For larger d, the correct dyadic range satisfies (95)–(96), and Lemma 4.1 supplies the first exact relation. Proposition 5.1 places every factor that can contain the target in a branch explored by the algorithm. The factors involving only z and the fixed-y factors give direct recovery, while Lemmas 7.1 and 7.2 handle the two lower-degree branches.

For a cubic factor, choose the fixed transition constant K large enough that (95) implies the lower bound on θ in Proposition 8.11. That proposition supplies a second relation outside (H_3), vanishing at the RSA root. The algorithm runs both cubic constructions and all admissible charts, so it includes the construction guaranteed by the proposition.

Thus every remaining branch contains two coprime fixed-degree equations. Resultant elimination lists their common zeros, and the verification procedure above identifies the target. The runtime and verification bounds follow from the preceding algorithmic analysis. This proves the theorem. □

10 Conclusion

We proposed a fully rigorous deterministic polynomial-time factoring algorithm for balanced RSA with $e = \Theta(N)$ and $d \leq N^{11/42-\varepsilon}$. The proof follows a single organizing principle: one exact relation is factored into relevant components, and for each component, we either recover the root directly or construct a second polynomial that vanishes at the RSA root and is coprime to the first one. Exact elimination and RSA verification then complete the algorithm.

Our work leaves two natural questions. The first is to extend our bound 11/42 toward the Boneh–Durfee exponent $1 - \sqrt{2}/2$. The second question is whether the same quotient and restriction technique applies to other multivariate Coppersmith settings whose root extraction is currently heuristic.

AI use disclosure

Large language model tools (Codex with GPT-5.6 sol) were used interactively at all stages of the preparation of this manuscript: from the earliest exploratory research stages to the final exposition and writing steps. The final manuscript was substantially revised by the authors, who take full responsibility for all mathematical claims, proofs, references, and conclusions.

References

[BD99] Dan Boneh and Glenn Durfee. Cryptanalysis of RSA with private key d less than $N^{0.292}$. In *Advances in Cryptology – EUROCRYPT '99*, volume 1592 of *Lecture Notes in Computer Science*, pages 1–11. Springer, 1999.

[BD00] Dan Boneh and Glenn Durfee. Cryptanalysis of RSA with private key $d < N^{0.292}$. *IEEE Transactions on Information Theory*, 46(4):1339–1349, 2000.

[BJ07] Aurélie Bauer and Antoine Joux. Toward a rigorous variation of Coppersmith's algorithm on three variables. In *Advances in Cryptology – EUROCRYPT 2007*, volume 4515 of *Lecture Notes in Computer Science*, pages 361–378. Springer, 2007.

[CLO15] David A. Cox, John Little, and Donal O'Shea. Elimination theory. In *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Undergraduate Texts in Mathematics, pages 121–174. Springer, Cham, 2015.

[Cop96a] Don Coppersmith. Finding a small root of a bivariate integer equation; factoring with high bits known. In *Advances in Cryptology – EUROCRYPT '96*, volume 1070 of *Lecture Notes in Computer Science*, pages 178–189. Springer, 1996.

[Cop96b] Don Coppersmith. Finding a small root of a univariate modular equation. In *Advances in Cryptology – EUROCRYPT '96*, volume 1070 of *Lecture Notes in Computer Science*, pages 155–165. Springer, 1996.

[HG97] Nick Howgrave-Graham. Finding small roots of univariate modular equations revisited. In *Cryptography and Coding (IMA 1997)*, volume 1355 of *Lecture Notes in Computer Science*, pages 131–142. Springer, 1997.

[HM10] Mathias Herrmann and Alexander May. Maximizing small root bounds by linearization and applications to small secret exponent RSA. In *Public Key Cryptography – PKC 2010*, volume 6056 of *Lecture Notes in Computer Science*, pages 53–69. Springer, 2010.

[HS07] Guillaume Hanrot and Damien Stehlé. Improved analysis of Kannan's shortest lattice vector algorithm. In *Advances in Cryptology – CRYPTO 2007*, volume 4622 of *Lecture Notes in Computer Science*, pages 170–186. Springer, 2007.

[LLL82] Arjen K. Lenstra, Hendrik W. Lenstra, Jr., and László Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261:515–534, 1982.

[MNV21] Stephen D. Miller, Bhargav Narayanan, and Ramarathnam Venkatesan. Coppersmith's lattices and "focus groups": An attack on small-exponent RSA. *Journal of Number Theory*, 222:376–392, 2021.

[MV10] Daniele Micciancio and Panagiotis Voulgaris. A deterministic single exponential time algorithm for most lattice problems based on Voronoi cell computations. In *Proceedings of the Forty-Second Annual ACM Symposium on Theory of Computing (STOC 2010)*, pages 351–358. ACM, 2010.

[Rya25] Keegan Ryan. Solving multivariate Coppersmith problems with known moduli. In *Advances in Cryptology – EUROCRYPT 2025*, volume 15606 of *Lecture Notes in Computer Science*, pages 355–384. Springer, 2025.

[Wie90] Michael J. Wiener. Cryptanalysis of short RSA secret exponents. *IEEE Transactions on Information Theory*, 36(3):553–558, 1990.