

Polynomial parametrizations for two classes of Diophantine equations

Bogdan Grechuk

26 October 2026

Abstract

We prove that the integer solution sets of two classes of Diophantine equations are finite unions of polynomial families with integer coefficients and unrestricted integer parameters. In the first class, each monomial, with at most one exception, contains a variable that occurs to the first power and in no other monomial. The second class consists of equations $M = f(t)$, where M is a monomial independent of t with a variable occurring to the first power, and $f \in \mathbb{Z}[t]$ splits completely over $\mathbb{Q}$. If M involves at most two variables, f may instead be an arbitrary quadratic polynomial. We also give complete formulas for five equations listed as open in the monograph *Polynomial Diophantine Equations: A Systematic Approach* (2024).

1 Introduction

For a polynomial Diophantine equation

$$P(x_1, \dots, x_n) = 0, \tag{1.1}$$

a natural goal is to describe all integer solutions by finitely many explicit formulas. Polynomial parametrizations provide a particularly useful form of such a description: every parameter choice produces a solution, and every solution is attained.

We use the terminology of [1] and [8, Definition 1.4].

Definition 1.2. A *polynomial family* in $\mathbb{Z}^n$ is the image of a map $\Phi \in \mathbb{Z}[t_1, \dots, t_\nu]^n$ evaluated at all of $\mathbb{Z}^\nu$, where $\nu \geq 0$. The map Φ is a *polynomial parametrization* of its image. A set $S \subseteq \mathbb{Z}^n$ is a *finite union of polynomial families* if $S = \bigcup_{j=1}^h \Phi_j(\mathbb{Z}^{\nu_j})$ for finitely many such maps. We allow $h = 0$, representing the empty set, and $\nu_j = 0$, representing a single point. The families need not be disjoint.

We ask when the integer solution set of (1.1) is a finite union of polynomial families. The coefficients in Definition 1.2 are integers, and the parameters are independent and unrestricted. Rational functions with variable denominators, or formulas with unresolved coprimality conditions, do not by themselves exhibit the solution set as a finite union of polynomial families.

This question can be difficult even for simple equations. The existence of a polynomial parametrization of

$$x_1x_2 - x_3x_4 = 1$$

was a longstanding open problem, resolved by Vaserstein [1, Theorem 1]. Chapter 2 of the monograph [8] uses this theorem to represent the solution sets of many other equations as

finite unions of polynomial families. Several small examples were left open there and appear in [9, Table 1], including

$$x^2y + zt + 1 = 0, \quad x_1x_2x_3 + x_4x_5 + 1 = 0, \quad (1.3)$$

$$x^2y + z^2 \pm 1 = 0, \quad xyz + t^2 - 1 = 0. \quad (1.4)$$

The present paper develops two general constructions that apply to these equations and supplies complete formulas and proofs in Section 8.

Our main results are the following two theorems. A monic monomial is $x^e = \prod_j x_j^{e_j}$ with nonnegative integer exponents; the constant monomial 1 is allowed.

Theorem A. *Let $M_0, \dots, M_s$ be monic monomials in $x = (x_1, \dots, x_n)$, with $s \geq 1$, and fix integers $\alpha_1, \dots, \alpha_s \neq 0$ and c . Let $y_1, \dots, y_s$ be distinct variables absent from every M_j ; the monomial supports may overlap arbitrarily. Then the integer solutions of*

$$\sum_{i=1}^s \alpha_i M_i(x) y_i = c M_0(x) \quad (1.5)$$

form a finite union of polynomial families.

Theorem B. *Fix $\kappa \in \mathbb{Z} \setminus \{0\}$, $f \in \mathbb{Z}[t]$, a nonnegative integer r , and positive integers $e_1, \dots, e_r$. Let $z, x_1, \dots, x_r, t$ be distinct variables. Then all integer solutions of*

$$\kappa z \prod_{i=1}^r x_i^{e_i} = f(t)$$

form a finite union of polynomial families if f splits completely over $\mathbb{Q}$, or if $r \leq 1$ and $\deg f \leq 2$. Constant and zero polynomials are included.

The first class in the abstract follows from Theorem A: in each non-exceptional monomial choose a variable that occurs to the first power and in no other monomial, call it y_i , and collect all remaining variables in x . Move the exceptional monomial to the right-hand side, or take $c = 0$ if there is none. Equations with at most one nonzero monomial are immediate: their solution sets are unions of coordinate hyperplanes, the empty set, or the whole space.

The equations in (1.3) are covered by Theorem A, and those in (1.4) by Theorem B. In the latter theorem, the arbitrary quadratic alternative allows only one powered variable in addition to the linear factor.

The proofs use Vaserstein's parametrization of $\mathrm{SL}_2(\mathbb{Z})$ [1, Theorem 1] and his factorization of congruence subgroups [1, Proposition 5.9 and Corollary 5.11]. Section 3 establishes the required polynomial dependence on the congruence level. We also use the representation of rational polynomial families as finite unions of polynomial families [2, Lemmas 2–3] (see also [8, Proposition 1.28]), and Gordan's lemma [4, Proposition 2.1.1(a)]. Related work of Frisch and Lettl [3, Theorem 1] gives integer-valued parametrizations for the affine cones over rational projective plane curves, apart from specified singular-point exceptions. Our constructions use coprime block products and valuation semigroups; for quadratic polynomials irreducible over $\mathbb{Q}$, we also use standard ideal arithmetic.

The paper is organized as follows. Section 2 collects polynomial operations and algebraic inputs. Section 3 adapts Vaserstein's published congruence parametrization to a variable level, including levels 0 and 1. Section 4 constructs polynomial parametrizations of pairwise coprime block products, together with polynomial Bézout identities. Section 5 proves Theorem A. Sections 6 and 7 prove the split and quadratic alternatives of Theorem B, respectively. Section 8 gives complete solution formulas for the five equations above.

2 Polynomial operations and algebraic inputs

We take empty products to be 1. Gcds are nonnegative, with $\gcd(0, n) = |n|$; a tuple is primitive (or unimodular) if its coordinates have gcd 1. For $a \neq 0$, $v_p(a)$ is the exponent of p in $|a|$. For a quadratic number field K , its ring of integers is $\mathcal{O}_K$, conjugation is $\alpha \mapsto \bar{\alpha}$, and $N(\alpha) = \alpha\bar{\alpha}$. Ideal norms extend multiplicatively from $N(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{a}]$, so $N((\alpha)) = |N(\alpha)|$.

For $P \in \mathbb{Q}[t_1, \dots, t_\nu]^n$, the set $P(\mathbb{Z}^\nu) \cap \mathbb{Z}^n$ is a *rational polynomial family* [8, Definition 1.27].

Lemma 2.1 (Fixed denominators and congruences). *Let $\mathbf{t} = (t_1, \dots, t_\nu)$ and $P \in D^{-1}\mathbb{Z}[\mathbf{t}]^n$, with $D \geq 1$ fixed. The integral values of P on $\mathbb{Z}^\nu$ satisfying finitely many fixed coordinate congruences form a finite union of polynomial families. The same holds for fixed congruences on integer-polynomial expressions in the retained coordinates and parameters. If $\Psi(\mathbf{t}, P(\mathbf{t})) = 0$ is a polynomial identity, it remains an identity after each residue-class substitution used to construct these families.*

Proof. This is the residue-class argument of [2, Lemmas 2–3]; the case without congruences is also [8, Proposition 1.28]. Let $m_0 > 0$ be a common multiple of the congruence moduli. For every $a \in \mathbb{Z}^\nu$, expansion gives

$$P(a + Dm_0\mathbf{u}) - P(a) \in m_0\mathbb{Z}[\mathbf{u}]^n.$$

Thus integrality and the required residues depend only on $a \bmod Dm_0$. On each admissible class, $P(a + Dm_0\mathbf{u})$ has integer coefficients. The finitely many admissible classes give exactly the desired values. For auxiliary expressions, append them as extra coordinates, enlarge D if necessary, apply the same argument, and project to the desired coordinates. $\square$

Remark 2.2 (Polynomial quotients). An expression such as $(A - a)/P$ below denotes a quotient proved to lie in the integer polynomial ring, *before* parameter specialization. For example, if a construction gives $A - a = P^2H$, we define $(A - a)/P = PH$. It then has value zero when $P = 0$. All parameter substitutions are allowed, including those at which a displayed polynomial denominator vanishes. Congruences between polynomials mean ideal divisibility in their polynomial ring.

2.1 Bézout identities

For $A, B \in \mathcal{R} = \mathbb{Z}[\mathbf{u}]$, we use Bézout coefficients $R, S \in \mathcal{R}$ satisfying $AR + BS = 1$ as a polynomial identity. For a tuple $(A_1, \dots, A_s)$, the corresponding identity is $\sum_i A_i R_i = 1$ with $R_i \in \mathcal{R}$. These identities mean that the polynomials generate the unit ideal; having no common nonunit factor alone would not suffice. The following elementary identities will be used repeatedly. From $AR + BS = 1$ and $A' = A + BH$ one obtains

$$A'R + B(S - RH) = 1. \tag{2.3}$$

From $AR + BS = 1$ and $AU + CV = 1$ one obtains

$$A(R + U - ARU) + BCSV = 1. \tag{2.4}$$

The second identity follows by expanding $(1 - AR)(1 - AU) = BCSV$. It combines the identities for (A, B) and (A, C) into one for (A, BC) ; swapping the two roles gives the analogous operation for a product in the first slot. If $A = A_1A_2$, a Bézout identity for (A, B) gives one for (A_1, B) by replacing R with A_2R .

The same Bézout identity gives an inverse modulo a square:

$$A(R(2 - AR)) = 1 - B^2S^2. \tag{2.5}$$

Thus all inverses modulo variable squares used later are polynomials, not chosen numerical inverse functions.

Lemma 2.6 (Raising prescribed powers). *If $X = \prod_i x_i$, $Y = \prod_j y_j$ and $XR + YS = 1$ polynomially, then $A = \prod_i x_i^{e_i}$ and $B = \prod_j y_j^{f_j}$ have polynomial Bézout identities for any fixed positive exponents.*

Proof. For nonempty products put $E = \max_i e_i$, $F = \max_j f_j$. Expand $1 = (XR + YS)^{E+F-1}$: every term is divisible by A or by B , so grouping terms gives the Bézout identities. An empty product equals 1. $\square$

2.2 A congruence-compatible matrix completion

Lemma 2.7 (Lifting a primitive column). *Let $m_0 > 0$ and $H_0 \in \mathrm{SL}_2(\mathbb{Z})$. If the primitive column $(a, c)^T$ is congruent modulo m_0 to the first column of H_0 , it has a completion $H_1 \in \mathrm{SL}_2(\mathbb{Z})$ satisfying $H_1 \equiv H_0 \pmod{m_0}$.*

Proof. Choose any determinant-one completion H of $(a, c)^T$. Modulo m_0 the matrix $H^{-1}H_0$ has first column $(1, 0)^T$ and determinant 1, so it has form $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$. Choose an integer representative of h and set $H_1 = H \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$. This preserves the first column and gives the required congruence. For $m_0 = 1$ the condition is vacuous and the proof still applies. $\square$

Lemma 2.8 (Gordan's lemma [4, Proposition 2.1.1(a)]). *For a rational polyhedral cone $C \subseteq \mathbb{R}_{\geq 0}^n$, the additive monoid $C \cap \mathbb{Z}^n$ has finitely many generators.*

Lemma 2.9 (Solutions of a linear equation). *Let $s \geq 1$, let $\mathbf{t} = (t_1, \dots, t_\nu)$, and suppose $A_i, R_i, H \in \mathbb{Z}[\mathbf{t}]$ satisfy $\sum_{i=1}^s A_i R_i = \Lambda$, where $\Lambda > 0$ is fixed. The set*

$$\left\{ (\mathbf{t}, \mathbf{y}) \in \mathbb{Z}^\nu \times \mathbb{Z}^s : \sum_{i=1}^s A_i(\mathbf{t}) y_i = H(\mathbf{t}) \right\}$$

is a finite union of polynomial families. More explicitly, it consists of the integral values of the map $(\mathbf{t}, \mathbf{v}) \mapsto (\mathbf{t}, \mathbf{y})$ defined by

$$y_i = \frac{H R_i}{\Lambda} + v_i - \frac{R_i}{\Lambda} \sum_{j=1}^s A_j v_j, \quad \mathbf{v} = (v_1, \dots, v_s) \in \mathbb{Z}^s, \quad (2.10)$$

with $\mathbf{t} \in \mathbb{Z}^\nu$.

Proof. Summing verifies the equation. For any prescribed solution take $v_i = y_i$; the formula returns the target. Lemma 2.1 retains integral outputs and removes the fixed denominator Λ . $\square$

3 A polynomial congruence map with variable level

Vaserstein's Theorem 13 parametrizes each fixed principal congruence subgroup. We need polynomial dependence on the level as well. We prove this from his fixed factorization in [1, Proposition 5.9].

3.1 Polynomial matrices

Put

$$U(v) = \begin{pmatrix} 1 & v \\ 0 & 1 \end{pmatrix}, \quad L(v) = \begin{pmatrix} 1 & 0 \\ v & 1 \end{pmatrix}, \quad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Let $D_j(v_1, \dots, v_j)$ be the alternating product of j elementary matrices beginning with $U(v_1)$, and let C_j begin with $L(v_1)$. These are Vaserstein's polynomial matrices Δ_j, Γ_j , respectively.

We use the following explicit versions of his polynomial matrices from [1, Section 1, definitions preceding Lemma 1.1]:

$$F(a, c) = \begin{pmatrix} 1 - ac & a^2 \\ -c^2 & 1 + ac \end{pmatrix}, \quad \Phi_4(a, b, c, d) = F(b, d)F(a, c)F(b, d)J^{-1}. \quad (3.1)$$

Every factor has determinant 1, and $\Phi_4(1, 0, 0, 1) = I_2$. If $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ has determinant 1, conjugating $L(-1)U(1)L(-1) = J$ by α gives

$$\Phi_4(a, b, c, d) = \alpha\alpha^T. \quad (3.2)$$

For five free arguments define

$$W = \Phi_4(1 + ae, be, ce, 1 + de), \quad \Phi_5(a, b, c, d, e) = \begin{pmatrix} W_{11} & eW_{12} \\ W_{21}/e & W_{22} \end{pmatrix}. \quad (3.3)$$

Here $W|_{e=0} = I_2$, so W_{21}/e is an integer polynomial, defined also at $e = 0$. The determinant identity for W gives $\det \Phi_5 = 1$ as a polynomial identity.

With q an indeterminate and all v_i free, set

$$\begin{aligned} D_j(q; \mathbf{v}) &= D_j(qv_1, \dots, qv_j), & C_j(q; \mathbf{v}) &= C_j(qv_1, \dots, qv_j), \\ \widehat{X}_4(q; \mathbf{v}) &= \Phi_4(1 + q^2v_1, qv_2, qv_3, 1 + q^2v_4), \\ \widehat{X}_5(q; \mathbf{v}) &= \Phi_5(q^2v_1, qv_2, qv_3, q^2v_4, v_5), & \widehat{Y}_5(q; \mathbf{v}) &= \widehat{X}_5(q; \mathbf{v})^T. \end{aligned} \quad (3.4)$$

All entries belong to $\mathbb{Z}[q, \mathbf{v}]$. To check their congruences, expand (3.1) modulo q^2 :

$$\widehat{X}_4 \equiv \begin{pmatrix} 1 & q(v_2 + v_3) \\ q(v_2 + v_3) & 1 \end{pmatrix}, \quad \widehat{X}_5 \equiv \begin{pmatrix} 1 & qv_5^2(v_2 + v_3) \\ q(v_2 + v_3) & 1 \end{pmatrix} \pmod{q^2}.$$

For the lower-left entry of the second matrix, the remainder before division is divisible by both q^2 and v_5 , hence by q^2v_5 . The elementary products have the same diagonal and off-diagonal divisibilities, since these are preserved under multiplication. Consequently every matrix takes values in

$$G(q) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : q \mid b, c, \quad q^2 \mid a - 1, d - 1 \right\} \quad (q \geq 2),$$

and every matrix is I_2 at $q = 0$.

3.2 Coverage of the fixed factorization

The sets $X_4(q), X_5(q), Y_5(q)$ in Vaserstein's Proposition 5.9 are contained in the respective images in (3.4). Indeed, $X_4(q)$ consists of $\alpha\alpha^T$ with $\alpha \in G(q)$. Equation (3.2) gives the inclusion by taking the four free arguments to be the normalized entries of α .

An element of $X_5(q)$ has the form

$$\begin{pmatrix} 1 + aq^2e & bqe^2 \\ cq & 1 + dq^2e \end{pmatrix} \begin{pmatrix} 1 + aq^2e & cqe^2 \\ bq & 1 + dq^2e \end{pmatrix}, \quad (3.5)$$

where the first matrix has determinant 1. The entry cqe^2 in the second factor follows from [1, Section 1]; the extra factor q printed on p. 1000 appears to be a misprint. For $e \neq 0$, put $D_e = \mathrm{diag}(e, 1)$ and $\alpha = \begin{pmatrix} 1 + aq^2e & bqe \\ cqe & 1 + dq^2e \end{pmatrix}$. The two factors in (3.5) are $D_e\alpha D_e^{-1}$ and $D_e\alpha^T D_e^{-1}$. Since $\det \alpha = 1$, (3.2)–(3.3) give

$$D_e\alpha\alpha^T D_e^{-1} = \Phi_5(aq^2, bq, cq, dq^2, e) = \widehat{X}_5(q; a, b, c, d, e).$$

At $e = 0$ the product in (3.5) is $L(q(b+c))$. Here the same arguments cannot in general be used, since

$$\widehat{X}_5(q; a, b, c, d, 0) = L(q(b+c) - 2q^2(a+d)).$$

Instead, the preimage $(0, b, c, 0, 0)$ gives $L(q(b+c))$. Replacing (a, b, c, d) by $(d, -c, -b, a)$ reverses and inverts the two factors, so $X_5(q)$ is closed under inversion. Hence Vaserstein's $Y_5(q) = (X_5(q)^{-1})^T$ is covered by $\widehat{Y}_5$.

Suppressing the level and the free arguments, form the following polynomial matrix, with independent arguments at each occurrence:

$$\begin{aligned} \mathcal{P}(q; \theta) = & C_6 \widehat{X}_5 D_4 \widehat{Y}_5 C_6 \widehat{X}_5 C_6 \widehat{X}_4 \\ & \cdot C_5 \widehat{Y}_5 C_4 \widehat{X}_5 D_6 \widehat{Y}_5 D_6 \widehat{X}_4 \\ & \cdot C_3 \widehat{X}_5 D_2 \widehat{X}_5 U(q) \widehat{Y}_5 C_2. \end{aligned} \quad (3.6)$$

The elementary products use 50 parameters, the nine five-parameter matrices use 45, and the two four-parameter matrices use 8. Thus $\theta \in \mathbb{Z}^{103}$. For each integer $q \geq 2$, [1, Proposition 5.9] expresses every element of $G(q)$ as this word in the original sets. The inclusions just proved supply preimages in our free polynomial matrices. Conversely, every factor in our word belongs to $G(q)$. Hence

$$\mathcal{P}(q; \mathbb{Z}^{103}) = G(q) \quad (q \geq 2). \quad (3.7)$$

The primes and exponents chosen in the proof of that proposition determine preimages in its factor sets. The fixed maps (3.4) and word (3.6) give joint polynomial dependence on the level and the parameters. We use the resulting 103-parameter map; Vaserstein obtains smaller counts for fixed levels in [1, Corollaries 5.10–5.11].

3.3 The full congruence subgroup and levels zero and one

Set $\Gamma(0) = \{I_2\}$ and $\Gamma(q) = \{g \in \mathrm{SL}_2(\mathbb{Z}) : g \equiv I_2 \pmod{q}\}$ for $q > 0$. For a free integer h put

$$T(q, h) = L(1)U(qh)L(-1) = \begin{pmatrix} 1 - qh & qh \\ -qh & 1 + qh \end{pmatrix}, \quad Q(q; \theta, h) = \mathcal{P}(q; \theta)T(q, h).$$

Then $Q \in \mathrm{SL}_2(\mathbb{Z}[q, \theta, h])$, $Q - I_2$ is divisible by q , and $Q(q; \mathbb{Z}^{104}) = \Gamma(q)$ for $q \geq 2$. To see surjectivity, write the diagonal of $g \in \Gamma(q)$ as $(1 + q\lambda, 1 + q\mu)$. Its determinant gives $\lambda + \mu \equiv 0 \pmod{q}$. Choose $h \equiv -\lambda \pmod{q}$. The diagonal of $gT(q, h)^{-1}$ is then $(1, 1)$ modulo q^2 , so this matrix belongs to $G(q)$ and is attained in (3.7). This verifies directly the extra-parameter step underlying [1, Corollary 5.11].

Fix a matrix $V(\xi) \in \mathrm{SL}_2(\mathbb{Z}[\xi_1, \dots, \xi_{46}])$ parametrizing $\mathrm{SL}_2(\mathbb{Z})$ by [1, Theorem 1]. Replacing it by $V(\xi)V(0)^{-1}$ ensures $V(0) = I_2$.

Lemma 3.8 (Uniform congruence parametrization). *There is $K \in \mathrm{SL}_2(\mathbb{Z}[q, \vartheta_1, \dots, \vartheta_{150}])$ such that $K - I_2$ is polynomially divisible by q and $K(q; \mathbb{Z}^{150}) = \Gamma(q)$ for every integer $q \geq 0$.*

Proof. For $\vartheta = (\theta, h, \xi)$ define

$$K(q; \vartheta) = Q(q; \theta, h)V(q\xi). \quad (3.9)$$

The determinant is 1 and $K - I_2$ is divisible by q in the integer polynomial ring. For $q \geq 2$, setting $\xi = 0$ gives the whole of $\Gamma(q)$ by the preceding argument. There is a fixed θ_* with $\mathcal{P}(q; \theta_*) = I_2$ identically: set all arguments to zero except the second argument of the final C_2 , which is -1 . The remaining factors are $U(q)U(-q)$. At $q = 1$, take $\theta = \theta_*$ and $h = 0$; then $K = V(\xi)$. At $q = 0$, every factor is I_2 . $\square$

4 Pairwise coprime block products

The next construction replaces coprimality conditions by unrestricted polynomial parameters. All identities in this section take place in an integer polynomial ring. In particular, inverses modulo a variable polynomial are supplied by Bézout identities.

Lemma 4.1 (Insertion with preserved congruences). *Let $\mathcal{R} = \mathbb{Z}[s_1, \dots, s_N]$. Suppose $a, B, F, P, Q, w, \rho, \sigma, \iota_P, \iota_w, v, h_0 \in \mathcal{R}$, with $P = BF$, satisfy*

$$a\rho + P\sigma = 1, \quad P\iota_P \equiv w\iota_w \equiv 1 \pmod{Q^2}, \quad Qv + Bh_0 = 1. \quad (4.2)$$

Suppose also that B and w have a polynomial Bézout identity. With additional unrestricted parameters $\theta \in \mathbb{Z}^{150}$ and $\tau \in \mathbb{Z}$, one can construct $A, u, \rho', \sigma' \in \mathcal{R}[\theta, \tau]$ such that

$$\begin{aligned} A\rho' + Pu\sigma' &= 1, \\ u &\equiv w \pmod{B^2}, \quad u \equiv w \pmod{Q^2}. \end{aligned} \quad (4.3)$$

All congruences here are ideal congruences in the integer polynomial ring. The output pairs (u, B) and (u, Q) have polynomial Bézout identities. For every integer specialization of $s_1, \dots, s_N$ at which $\gcd(a, Pw) = 1$, there is $(\theta, \tau) \in \mathbb{Z}^{151}$ giving $A = a$ and $u = w$, including when $P = 0$ or $Q = 0$.

Proof. The elementary product $\mathcal{D}(s, t) = U(s-1)L(1)U(t-1)L(-s)$ equals $\text{diag}(s, t)$ modulo $st-1$. Set $\lambda = P^2\iota_P^2$ and

$$E = U(\lambda a \iota_w)U(\lambda(P\iota_w - 1))L(\lambda)U(\lambda(w\iota_P - 1))L(-\lambda P\iota_w)U(-\lambda a \iota_P). \quad (4.4)$$

Then $E \equiv I_2 \pmod{P^2}$. Modulo Q^2 it equals $U(a\iota_w)\mathcal{D}(P\iota_w, w\iota_P)U(-a\iota_P)$, which sends $(a, P)^T$ to $(a, w)^T$. Define

$$H = \begin{pmatrix} a & -\sigma \\ P & \rho \end{pmatrix}, \quad EHK((PQ)^2; \theta) = \begin{pmatrix} A & B_0 \\ C & D \end{pmatrix}, \quad (4.5)$$

using the polynomial matrix of Lemma 3.8. Consequently $(A, C) \equiv (a, P) \pmod{P^2}$ and $(A, C) \equiv (a, w) \pmod{Q^2}$.

The construction makes $A - a$ polynomially divisible by P^2 . Thus $h = (A - a)/P$ is an integer polynomial even at $P = 0$, and $\sigma_0 = \sigma - \rho h$ satisfies $A\rho + P\sigma_0 = 1$. Put

$$\begin{aligned} \zeta &= (v(2 - Qv))^2, & \iota_A &= \rho(2 - A\rho), \\ \chi &= Q^2((w - P)\iota_A\zeta + B^2\tau), & u &= C + \chi A, \quad D_0 = D + \chi B_0, \end{aligned} \quad (4.6)$$

where τ is free. Formula (2.5) gives $A\iota_A \equiv 1 \pmod{B^2}$ and $Q^2\zeta \equiv 1 \pmod{B^2}$. It follows that $u \equiv w \pmod{B^2}$; the congruence modulo Q^2 is immediate. The determinant identity is $AD_0 - uB_0 = 1$. Therefore

$$\rho' = \rho + P\sigma_0 D_0, \quad \sigma' = -\sigma_0 B_0$$

satisfy $A\rho' + Pu\sigma' = 1$. Writing $w\iota_w - 1 = Q^2 s_w$ gives $w\iota_w - Q(Qs_w) = 1$. Thus (w, Q) has a Bézout identity, as does (w, B) by hypothesis. Formula (2.3) transfers these identities to (u, Q) and (u, B) .

For coverage, first assume $PQ \neq 0$. At the target value $A = a$, let $\chi_0 = Q^2(w - P)\rho(2 - a\rho)\zeta$. The inverse identities give $w - a\chi_0 \equiv P \pmod{B^2}$. Choose τ such that

$$c = w - a\chi_0 - aQ^2 B^2 \tau \equiv P \pmod{P^2}, \quad P^2 = B^2 F^2.$$

After division by B^2 this is soluble modulo F^2 , because $\gcd(aQ, P) = 1$. We also have $c \equiv w \pmod{Q^2}$ and $\gcd(a, c) = \gcd(a, w) = 1$. The first column $(a, c)^T$ is therefore primitive and congruent to that of EH modulo $(PQ)^2$. Lemma 2.7 and the surjectivity of $K((PQ)^2)$ supply a matrix in (4.5) with that column. The final shear then gives $u = w$.

If $P = 0$, the input identities force $a, Q \in \{1, -1\}$ and $a\rho = 1$. Also $E = I_2$ and $K(0) = I_2$. Hence $A = a$, $C = 0$, and $u = w\zeta + aB^2\tau$. If $B = 0$, then $Qv = 1$ and $\zeta = 1$. If $B \neq 0$, then $\zeta \equiv 1 \pmod{B^2}$, so a choice of τ again gives $u = w$. Finally, if $Q = 0$, then $P\iota_P = w\iota_w = 1$; the matrix E sends $(a, P)^T$ exactly to $(a, w)^T$, while $K(0) = I_2$ and $\chi = 0$. The two zero cases cannot occur together. $\square$

Proposition 4.7 (Pairwise coprime products). *Partition N coordinates into blocks $I_1, \dots, I_h$, and put $X_j(x) = \prod_{\nu \in I_j} x_\nu$. There is an integer-polynomial map Φ on unrestricted integer parameters whose image is exactly*

$$\{x \in \mathbb{Z}^N : \gcd(X_i(x), X_j(x)) = 1 \text{ for } i < j\}.$$

There are also polynomial outputs R_{ij}, S_{ij} such that $X_i(\Phi)R_{ij} + X_j(\Phi)S_{ij} = 1$ identically for every $i < j$.

Proof. For two singleton blocks, the assertion follows from [1, Theorems 1 and 2.2]. We construct the map for arbitrary block sizes, including the condition $\gcd(x_1x_2, x_3) = 1$.

Induct on the total number of coordinates, filling the blocks in order. The first block has unrestricted coordinates; empty blocks have product 1 and trivial Bézout coefficients. The induction hypothesis supplies a polynomial map onto all tuples in the old blocks, together with polynomial Bézout coefficients for each pair of block products. Write these products as $X_1, \dots, X_g, Z$, where Z belongs to the block currently being filled. Adjoining a new coordinate keeps the coordinates of that block fixed and replaces those in blocks $1, \dots, g$ by new polynomials. Start the new coordinate as a free parameter a and initialize $P = 1$, $\rho = 0$, $\sigma = 1$, so $a\rho + P\sigma = 1$.

Process the coordinates of blocks $1, \dots, g$ in order. At an old coordinate w of block j , let B be the product of the completed new blocks and let F be the product of the processed new coordinates in the current block. Put

$$P = BF, \quad Q = Z \prod_{\ell > j} X_\ell,$$

where future blocks retain their old coordinates. The invariants at this step are:

- (i) every processed coordinate is congruent to its old value modulo the current Q^2 ;
- (ii) B is congruent to its old product modulo X_j^2 , and hence modulo w^2 ;
- (iii) $a\rho + P\sigma = 1$ is a polynomial identity.

At an earlier step in block $j' \leq j$, the modulus was $Q_{j'} = Z \prod_{\ell > j'} X_\ell$, with Z and the future X_ℓ still the old polynomials. Since $Q_j \mid Q_{j'}$, the congruence modulo $Q_{j'}^2$ gives (i). For $j' < j$, also $X_j \mid Q_{j'}$; taking products over completed blocks gives (ii). Taking products of the congruences in (i) also gives $P \equiv P_{\text{old}} \pmod{Q^2}$, where P_{old} is the product of the corresponding old coordinates. These are ideal divisibilities and remain valid when a factor vanishes.

The original pairwise Bézout identities, factored and combined using (2.4), give Bézout identities between each old processed product and Q . Transfer them by (2.3) and invariant (i). This explicitly supplies polynomial identities

$$Pr_P + Qs_P = 1, \quad wr_w + Qs_w = 1, \quad Qv + Bh_0 = 1.$$

Set

$$\iota_P = r_P(2 - Pr_P), \quad \iota_w = r_w(2 - wr_w).$$

Equation (2.5) gives the required inverses modulo Q^2 . Invariant (ii), the old pairwise Bézout identities and (2.3) also give a Bézout identity for (B, w) . Together with invariant (iii), these are all the inputs to Lemma 4.1. Apply it, replace a by A , and replace P by Pu after recording the new coordinate u . The conclusion maintains (iii). Its congruences modulo Q^2 and B^2 maintain (i)–(ii) as we move through the current block and then pass to the next block.

Write X'_i for the new completed block products. For $i < j$, the protected congruences give

$$X'_i \equiv X_i \pmod{X_j^2}, \quad X'_j \equiv X_j \pmod{(X'_i)^2}.$$

Applying (2.3) twice gives a Bézout identity for (X'_i, X'_j) . Also $X'_i \equiv X_i \pmod{Z^2}$, so (X'_i, Z) has a Bézout identity. The final identity $a\rho + (\prod_i X'_i)\sigma = 1$ gives a Bézout identity for (X'_i, a) ; combining these gives one for (X'_i, Za) . Thus all the new block products are pairwise coprime.

For a prescribed target, the old coordinates satisfy the induction hypothesis, so choose old parameters attaining them. Set a equal to the desired new coordinate. At every insertion the target satisfies $\gcd(a, Pw) = 1$. The coverage part of Lemma 4.1 retains a and the old value w . Hence the final output is the entire target. This proves surjectivity at the induction step. Every operation is polynomial, so zero coordinates are included throughout. $\square$

5 Proof of Theorem A: monomial coefficients

Lemma 5.1 (Monomials omitting a block). *Suppose the products $P_1, \dots, P_h$ of disjoint blocks of polynomial coordinates have polynomial pairwise Bézout identities. Let $B_1, \dots, B_s$, with $s \geq 1$, be monomials with coefficients 1 or -1 in these coordinates. Suppose that for each block j at least one $B_{i(j)}$ contains no coordinate of block j . Then $B_1, \dots, B_s$ have polynomial Bézout identities.*

Proof. If there are no blocks, every B_i is 1 or -1 , so the result is immediate. Otherwise choose a fixed $E \geq 1$ at least as large as every exponent in every B_i . Set $Q_j = P_j^E$ and $C_j = \prod_{\ell \neq j} Q_\ell$. Raising powers and combining pairwise Bézout identities gives $1 = U \prod_{\ell < h} Q_\ell + V Q_h$. The complements C_j generate the unit ideal by induction, starting with the single-block complement 1. For the induction step, if $1 = \sum_{j < h} W_j \prod_{\ell < h, \ell \neq j} Q_\ell$, substitute this identity in the term $V Q_h$ of the preceding identity. The result is a polynomial combination of all C_j . Each C_j is a monomial multiple of $B_{i(j)}$; substituting those formal monomial quotients yields the desired Bézout identities. The argument is an identity in a polynomial ring, so it does not exclude zeros. $\square$

Proof of Theorem A. Absorb the fixed α_i into the variables y_i and impose their divisibilities at the end. First take a target with every $x_j \neq 0$, and let $e_0, e_1, \dots, e_s$ be the monomial exponent vectors. For each coefficient index $1 \leq i \leq s$, define

$$E_i = \{v \geq 0 : (e_j - e_i) \cdot v \geq 0 \ (1 \leq j \leq s)\}.$$

If $c = 0$, put $C_i = E_i$; these cones cover the nonnegative orthant. If $c \neq 0$, put $C_i = E_i \cap \{v : (e_0 - e_i) \cdot v \geq 0\}$. For $c \neq 0$, solvability after absorbing the α_i requires $\gcd_i M_i(x) \mid cM_0(x)$. Thus, for the target valuation vector $v = (v_p(x_1), \dots, v_p(x_n))$,

$$\min_{1 \leq i \leq s} e_i \cdot v \leq e_0 \cdot v + v_p(c).$$

At every prime $p \nmid c$, this places v in some C_i . At $p \mid c$, with $\mu = v_p(c)$, it places v in some

$$\mathcal{A}_i(\mu) = E_i \cap \{v : (e_0 - e_i) \cdot v \geq -\mu\}.$$

There is a finite set $F_i(\mu) \subseteq \mathbb{Z}_{\geq 0}^n$ with

$$\mathcal{A}_i(\mu) \cap \mathbb{Z}^n = \bigcup_{b \in F_i(\mu)} (b + (C_i \cap \mathbb{Z}^n)). \quad (5.2)$$

Indeed, homogenize the last inequality to $(e_0 - e_i) \cdot v + \mu t \geq 0$, $t \geq 0$, and apply Gordan's lemma. The slice $t = 0$ is exactly C_i , so the generators with last coordinate zero generate $C_i \cap \mathbb{Z}^n$. Take $F_i(\mu)$ to be the projections of the generators with last coordinate one. In a decomposition with $t = 1$, exactly one generator has last coordinate one and all others have last coordinate zero. Conversely, $b + C_i \subseteq \mathcal{A}_i(\mu)$ for every $b \in F_i(\mu)$.

For each prime divisor of nonzero c , choose an index and a base vector from the finite sets above and put $h_j = \prod_{p|c} p^{b_{p,j}}$. For $c = 0$, take every $h_j = 1$. Set $x_j = h_j X_j$. Choose generators $g_{i,\ell}$ of the additive monoids $C_i \cap \mathbb{Z}^n$. Parametrize their variable blocks $(u_{i,\ell})_\ell$ with pairwise coprime block products using Proposition 4.7. For each of the finitely many signs $\varepsilon_j \in \{-1, 1\}$, write $\varepsilon^e = \prod_j \varepsilon_j^{e_j}$ and set

$$\begin{aligned} X_j &= \varepsilon_j \prod_{i,\ell} u_{i,\ell}^{(g_{i,\ell})_j}, & G &= \prod_{i,\ell} u_{i,\ell}^{e_i \cdot g_{i,\ell}}, \\ B_j &= \varepsilon^{e_j} \prod_{i,\ell} u_{i,\ell}^{(e_j - e_i) \cdot g_{i,\ell}} \quad (1 \leq j \leq s). \end{aligned}$$

If $c \neq 0$, also set $D = \varepsilon^{e_0} \prod_{i,\ell} u_{i,\ell}^{(e_0 - e_i) \cdot g_{i,\ell}}$; if $c = 0$, set $D = 0$. All exponents are nonnegative, and $M_j(X) = GB_j$, with $M_0(X) = GD$ when $c \neq 0$. For block i , B_i omits that block, so Lemma 5.1 supplies $\sum_j B_j W_j = 1$. With $H = cM_0(h)D$, apply Lemma 2.9 with $\Lambda = 1$ to obtain

$$Y_j = HW_j + v_j - W_j \sum_k B_k v_k, \quad y_j = Y_j / (\alpha_j M_j(h)),$$

retaining the fixed divisibilities $\alpha_j M_j(h) \mid Y_j$ by Lemma 2.1. These give polynomial solutions even when some parameter values make $G = 0$.

For coverage, assign each prime of a target to a cone containing its residual valuation vector and decompose in its generators. Distinct cone blocks have disjoint prime supports. Choose all $u_{i,\ell} > 0$ for this preimage and put the signs in ε . Proposition 4.7 attains these parameters, recovering the target X with $G \neq 0$. Taking $v_j = \alpha_j M_j(h) y_j$ then recovers every y_j by formula (2.10).

Finally fix a zero pattern among the x_j and delete the vanishing coefficient monomials. If M_0 vanishes, use the $c = 0$ construction just given. If M_0 survives, use the same proof on the remaining nonzero coordinates. When no coefficient survives, either the right-hand side also vanishes and all y_i are free, or there are no targets in that pattern. The variables y_i belonging to deleted summands are free. Every deleted monomial vanishes identically once the specified zero coordinates are fixed. Consequently, outputs of a reduced family still solve the original equation if further coordinates vanish. The families are indexed by finitely many zero patterns, sign vectors, choices $(i_p, b_p)_{p|c}$ when $c \neq 0$, and residue classes from Lemma 2.1. $\square$

6 Proof of Theorem B: split polynomials

We first prove the completely split alternative, namely

$$\kappa z \prod_{i=1}^r x_i^{e_i} = f(t), \quad (6.1)$$

for fixed $\kappa \neq 0$ and $f \in \mathbb{Z}[t]$ split over $\mathbb{Q}$.

6.1 Monomial columns from Gordan's lemma

Fix $m \geq 1$ and positive e_i . The valuation vectors for

$$Z \prod_i P_i^{e_i} = F^m \quad (6.2)$$

form the monoid $\{(z, p_1, \dots, p_r, f) \in \mathbb{Z}_{\geq 0}^{r+2} : z + \sum_i e_i p_i = mf\}$. By Gordan's lemma it has a finite Hilbert basis, consisting of its indecomposable nonzero elements. Its only basis element with every $p_i = 0$ is $g_0 = (m, 0, \dots, 0, 1)$; write $\mathcal{G}$ for the other elements. With free u, v_g and signs $\varepsilon_i = \pm 1$, set

$$\begin{aligned} P_i &= \varepsilon_i \prod_{g \in \mathcal{G}} v_g^{g p_i}, & A &= \prod_{g \in \mathcal{G}} v_g^{g f}, \\ F &= uA, & Z &= \left(\prod_i \varepsilon_i^{e_i} \right) u^m \prod_{g \in \mathcal{G}} v_g^{g z}. \end{aligned} \quad (6.3)$$

For a nonzero target, decompose each prime valuation in the Hilbert basis. Choose $v_g > 0$, let ε_i carry the sign of P_i , and let u carry the sign of F . The equation then forces the sign of Z to be $(\prod_i \varepsilon_i^{e_i}) \text{sign}(u)^m$, as in (6.3). Thus every nonzero target is attained. Every $g \in \mathcal{G}$ has a positive p_i and positive f coordinate. Consequently a prime absent from all target P_i can be assigned entirely to u , leaving every v_g prime to it. For $r = 0$ the formulas are $F = u, Z = u^m$.

6.2 Normalizing distinct integral roots

First take

$$f(t) = \prod_{j=1}^{s_f} (t - r_j)^{m_j}, \quad (6.4)$$

where $s_f \geq 1$, the r_j are distinct integers, and $m_j > 0$. Write $d_f = \sum_j m_j$. If $s_f \geq 2$ set

$$\Delta_{\text{rt}} = \prod_{j < \ell} |r_j - r_\ell|, \quad B_{\text{rt}} = \Delta_{\text{rt}}^{d_f}; \quad (6.5)$$

if $s_f = 1$, set $\Delta_{\text{rt}} = B_{\text{rt}} = 1$. For the moment take a target of (6.1) with $f(t) \neq 0$. All z, x_i , and $F_j = t - r_j$ are then nonzero. Put

$$h_i = \gcd(|x_i|, B_{\text{rt}}), \quad x_i = h_i X_i, \quad H = \prod_i h_i^{e_i}.$$

The tuples $(h_1, \dots, h_r)$ belong to a finite set.

Lemma 6.6 (Allocation to separate root factors). *For the normalized target there are integers P_{ij} such that*

$$X_i = \prod_j P_{ij}, \quad \prod_i P_{ij}^{e_i} \mid F_j^{m_j}, \quad (6.7)$$

and each prime divides entries P_{ij} in at most one column j .

Proof. If a prime p does not divide Δ_{rt} , at most one F_j is divisible by p ; allocate all residual p -powers to that column. If $p \mid \Delta_{\text{rt}}$, put $\ell = v_p(\Delta_{\text{rt}})$. At most one of the $v_p(F_j)$ can exceed ℓ , since $F_j - F_{j'} = r_{j'} - r_j$ and each difference has valuation at most ℓ . Choose a column j of maximal valuation. If a residual X_i contains p , some original x_i has valuation greater than $d_f \ell$, and hence the total removed weighted valuation is at least $d_f \ell$. Therefore

$$\begin{aligned} \sum_i e_i v_p(X_i) &= \sum_h m_h v_p(F_h) - v_p(\kappa) - v_p(z) - \sum_i e_i \min(v_p(x_i), d_f \ell) \\ &\leq m_j v_p(F_j) + \sum_{h \neq j} m_h \ell - d_f \ell \leq m_j v_p(F_j). \end{aligned}$$

Allocate all residual powers at this prime to the single column j . If no residual X_i contains p , nothing is allocated. The allocations produce (6.7); signs can be distributed arbitrarily among the columns to give the prescribed signs of the X_i . $\square$

Put $Z_j = F_j^{m_j} / \prod_i P_{ij}^{e_i}$. Then

$$Z_j \prod_i P_{ij}^{e_i} = F_j^{m_j}, \quad \prod_j Z_j = \kappa H z. \quad (6.8)$$

Represent each column by (6.3). By its support property and Lemma 6.6, the blocks of non- g_0 parameters v_{jg} can be chosen with pairwise coprime block products. Their coefficient monomials

$$A_j = \prod_g v_{jg}^{g_f} \quad (6.9)$$

are therefore pairwise coprime, and $F_j = u_j A_j$.

6.3 The Chinese remainder theorem

Use Proposition 4.7 to parametrize the blocks $(v_{jg})_g$ so that their block products are pairwise coprime, with polynomial Bézout identities. By Lemma 2.6 and (2.4), for each j we can construct polynomial Bézout identities

$$A_j R_j + B_j S_j = 1, \quad B_j = \prod_{\ell \neq j} A_\ell. \quad (6.10)$$

For $s_f = 1$, use $B_1 = 1, R_1 = 0, S_1 = 1$. Let $\Pi = \prod_j A_j$ and introduce one free parameter w . Define

$$T_0 = \sum_j r_j B_j S_j, \quad T = T_0 + \Pi w, \quad (6.11)$$

$$u_j = -r_j R_j + \sum_{\ell \neq j} r_\ell \left(\prod_{h \neq \ell, j} A_h \right) S_\ell + B_j w. \quad (6.12)$$

Using (6.10), expansion gives the polynomial identities

$$T - r_j = A_j u_j \quad (1 \leq j \leq s_f). \quad (6.13)$$

The formulas contain no division by A_j and are valid when some $A_j = 0$. For a nonzero target representation all A_j are nonzero and pairwise coprime. The integer $t - T_0$ is divisible by each A_j , hence by their product, so some integer w makes $T = t$. The formulas then give exactly the target $u_j = (t - r_j)/A_j$.

Substitute these u_j in the parametrization (6.3) of each column. Retain the one fixed congruence

$$\prod_j Z_j \equiv 0 \pmod{\kappa H}. \quad (6.14)$$

After the finite parameter subdivision of Lemma 2.1, define

$$t = T, \quad x_i = h_i \prod_j P_{ij}, \quad z = \frac{\prod_j Z_j}{\kappa H}. \quad (6.15)$$

All these coordinates are integer polynomials. Multiplying (6.8) and using (6.13) proves the original equation for every parameter value. Conversely, the allocation and column representation above put every nonzero target in one of these families; its parameters satisfy

(6.14) because $\prod_j Z_j = \kappa H z$. The choices of h_i and the column sign vectors are finite. There are no remaining variable coprimality or divisibility conditions on the parameters.

For a target with $f(t) = 0$, fix t to one of its finitely many integral roots and fix one of z, x_i to zero. Leave all other variables free. These finitely many linear families cover the remaining targets.

6.4 Multipliers and rational roots

We first allow a fixed nonzero integer multiplier λ on the right:

$$\kappa z \prod_i x_i^{e_i} = \lambda p_0(t), \quad (6.16)$$

where p_0 is monic with integral roots as in (6.4). Targets with $p_0(t) = 0$ are covered by the linear root families above. For a target with $p_0(t) \neq 0$, set

$$h_0 = \gcd(|z|, |\lambda|), \quad h_i = \gcd(|x_i|, |\lambda|).$$

Among the finitely many divisor choices, retain those for which

$$\kappa' = \frac{\kappa h_0 \prod_i h_i^{e_i}}{\lambda} \quad (6.17)$$

is an integer. Every target supplies such a choice. Indeed, for $\mu = v_p(\lambda)$ the original equation gives

$$v_p(\kappa) + v_p(z) + \sum_i e_i v_p(x_i) \geq \mu.$$

Keep $v_p(\kappa)$ unchanged and truncate each coordinate valuation at μ . If no coordinate is truncated, the sum is unchanged; otherwise a truncated coordinate alone contributes at least μ . Thus $v_p(\kappa) + v_p(h_0) + \sum_i e_i v_p(h_i) \geq \mu$, proving that (6.17) is integral. Apply the result already proved to $\kappa' Z \prod_i X_i^{e_i} = p_0(t)$ and rescale $z = h_0 Z, x_i = h_i X_i$. Every output solves (6.16), and every target is covered. Coefficient signs cause no change to the argument.

Finally let $f \in \mathbb{Z}[t]$ split over $\mathbb{Q}$ and have degree $d_f > 0$ and leading coefficient $\lambda \neq 0$. Choose a positive common denominator d_{rt} for its rational roots, and put $v = d_{rt}t$. Then, for distinct integral r_j and positive multiplicities m_j ,

$$d_{rt}^{d_f} f(t) = \lambda \prod_j (v - r_j)^{m_j}.$$

Apply the preceding result with coefficient $d_{rt}^{d_f} \kappa$ on the left, retain the fixed congruence $v \equiv 0 \pmod{d_{rt}}$, and output $t = v/d_{rt}$ using Lemma 2.1. Every target and every output correspond under this substitution.

If $f = 0$, the solution set is the union of the coordinate hyperplanes $z = 0$ or $x_i = 0$, with t free. If f is a nonzero constant, there are finitely many choices for the present monomial variables (or none), and t is free. This proves the split alternative of Theorem B.

7 Proof of Theorem B: irreducible quadratics

It remains to treat quadratic polynomials irreducible over $\mathbb{Q}$. We use unique factorization of nonzero ideals [6, Corollary 3.20] and finiteness of the ideal class group [7, Theorem 14.16 and Corollary 14.18].

Lemma 7.1 (A divisor ideal with prescribed norm). *Let $k \geq 1$ and let Δ be a nonsquare integer. Set $K = \mathbb{Q}(\delta)$ with $\delta^2 = \Delta$, and let $\mathcal{O}$ be its full ring of integers. Suppose $x \neq 0$ and $x^k y = T^2 - \Delta$ with integers x, y, T . Set $B_\Delta = 4|\Delta|$, $d = \gcd(|x|, B_\Delta)$ and $X = |x|/d$. There is an integral ideal $\mathfrak{a}$ with*

$$N \mathfrak{a} = X, \quad \mathfrak{a}^k \mid (T + \delta). \quad (7.2)$$

Only the finitely many divisors d of the fixed B_Δ occur.

Proof. Put $\alpha = T + \delta$, so $\bar{\alpha} = T - \delta$ and $\alpha - \bar{\alpha} = 2\delta$. Neither α nor its norm is zero. Use ideal valuations normalized so a prime ideal has valuation 1 in itself.

At an inert or ramified rational prime p there is a single prime ideal $\mathfrak{p}$ above p , fixed by conjugation. Therefore $v_{\mathfrak{p}}(\alpha) = v_{\mathfrak{p}}(\bar{\alpha}) \leq v_{\mathfrak{p}}(2\delta)$. Multiplying by its residue degree gives $v_p(|N \alpha|) \leq v_p(|N(2\delta)|) = v_p(B_\Delta)$. Since $kv_p(x) \leq v_p(|N \alpha|)$, no such prime divides X .

At a split prime, write $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ and let $R_p \geq S_p$ be the two valuations of α , relabeling the ideals if necessary. The difference identity implies $S_p \leq v_p(B_\Delta)$: at the chosen prime the minimum of the valuations of $\alpha, \bar{\alpha}$ is at most that of 2δ , which is at most $v_p(B_\Delta)$. Write $v = v_p(x)$ and $m = v_p(B_\Delta)$. If $v > m$, then

$$R_p \geq kv - S_p \geq kv - m \geq k(v - m) = kv_p(X).$$

If $v \leq m$, there is nothing to allocate. For every prime of X put $\mathfrak{p}^{v_p(X)}$ at the side with the larger valuation into $\mathfrak{a}$. Split prime ideals have norm p , so this gives exactly (7.2). For $p \nmid B_\Delta$ the argument simply says that one side has valuation zero and all the required valuation lies on the other. $\square$

7.1 Finitely many ideal bases and two homogeneous forms

Proposition 7.3 (The equation $x^k Y = T^2 - \Delta$). *For every nonsquare integer Δ and every integer $k \geq 1$, the integer solutions of*

$$x^k Y = T^2 - \Delta$$

form a finite union of polynomial families.

Proof. Put $K = \mathbb{Q}(\delta)$, $\delta^2 = \Delta$, let $\mathcal{O}$ be its ring of integers, and put $B_\Delta = 4|\Delta|$. Choose a finite list of nonzero integral ideals $\mathfrak{c}$ representing all ideal classes of $\mathcal{O}$. For each choose a $\mathbb{Z}$ -basis ω_1, ω_2 of $\mathfrak{c}$ and a $\mathbb{Z}$ -basis η_1, η_2 of the fractional ideal $\mathfrak{c}^{-k}$. These are fixed rank-two lattices. Write $n = N \mathfrak{c} > 0$. For unrestricted integers a, b, u, v put

$$\gamma = a\omega_1 + b\omega_2, \quad \beta = u\eta_1 + v\eta_2.$$

Let $\ell : K \rightarrow \mathbb{Q}$ extract the coefficient of δ in the basis $(1, \delta)$. With a fixed common denominator $D > 0$, define integer homogeneous forms of degree k by

$$F(a, b) = D\ell(\gamma^k \eta_1), \quad G(a, b) = D\ell(\gamma^k \eta_2).$$

These forms have no common nonzero algebraic zero. Indeed, $\ell(z) = (\iota_1(z) - \iota_2(z))/(2\delta)$ for the two embeddings. The embedding matrix of the basis η_1, η_2 is invertible, so $F = G = 0$ forces $\iota_1(\gamma)^k = \iota_2(\gamma)^k = 0$. The embedding matrix of ω_1, ω_2 then gives $a = b = 0$.

We need to express the solution set of the single coefficient equation

$$F(a, b)u + G(a, b)v = D \quad (7.4)$$

as a finite union of polynomial families. Homogeneity shows that $e^k \mid D$, where $e = \gcd(a, b) > 0$. There are finitely many such e . Write $a = eA, b = eB$ and parametrize primitive (A, B)

with a polynomial Bézout identity $Ap + B\sigma = 1$ using [1, Theorem 1]. The homogeneous resultant $\text{Res}(F, G)$ is nonzero, since F, G have no common projective zero [5, Chapter 3]. Put $\Lambda = |\text{Res}(F, G)|$ and $m = 2k - 1$. The adjugate of the Sylvester matrix, applied to the coefficient vectors of a^m and b^m , gives

$$\Lambda a^m, \Lambda b^m \in (F(a, b), G(a, b)) \mathbb{Z}[a, b].$$

Substitute the polynomial pair (A, B) and expand $1 = (Ap + B\sigma)^{2m-1}$. Each term is divisible by A^m or B^m , so Λ belongs to the substituted ideal. Lemma 2.9, with right-hand side D/e^k , now gives every solution (u, v) . Scaling back yields the required finite union of polynomial families for (7.4). On every family write $\gamma^k \beta = T + \delta$, where T is a rational polynomial with a fixed denominator. For each positive divisor $d \mid B_\Delta$ and each $\varepsilon \in \{-1, 1\}$ define

$$x = \varepsilon d \frac{N\gamma}{n}, \quad Y = \varepsilon^k \frac{n^k N\beta}{d^k}. \quad (7.5)$$

The forms $N\gamma/n$ and $n^k N\beta$ are integer quadratic polynomials. For the first assertion, $(\gamma) \subseteq \mathfrak{c}$ implies that the norm of each integer linear combination of the basis elements is divisible by n . Applying this to $(a, b) = (1, 0)$, $(0, 1)$ and $(1, 1)$ verifies divisibility of its three coefficients. The same argument with $(\beta)\mathfrak{c}^k \subseteq \mathcal{O}$ proves the second assertion, including the fractional ideal basis. Retain the fixed integrality conditions on T, Y and eliminate them by Lemma 2.1. Equations (7.5) and (7.4) then give unrestricted integer polynomials with

$$x^k Y = (N\gamma)^k N\beta = T^2 - \Delta.$$

To prove coverage, take an arbitrary target (x, Y, T) , put $\alpha = T + \delta$, and take the ideal $\mathfrak{a}$ from Lemma 7.1. Choose the representative $\mathfrak{c}$ whose class is inverse to that of $\mathfrak{a}$. Then $\mathfrak{a}\mathfrak{c} = (\gamma)$ is principal. It is contained in $\mathfrak{c}$, so its generator has the form $a\omega_1 + b\omega_2$ with integers a, b . Its norm satisfies $|N\gamma| = nX$. Since $\mathfrak{a}^k \mid (\alpha)$, the element $\beta = \alpha/\gamma^k$ belongs to $\mathfrak{c}^{-k}$, and therefore has integer coordinates u, v in its fixed basis. Its coefficient equation is exactly (7.4). Choose ε so that the first formula in (7.5) equals the target signed x . The norm identity then forces the output Y to equal the target value, because $x \neq 0$. All the fixed integrality conditions hold for these target data, so the polynomial families attain every target.

There is no omitted branch $x = 0$: a nonsquare Δ makes $T^2 - \Delta \neq 0$. Conversely (7.4) prevents $\gamma = 0$ at integer parameter values. Nonprincipal ideals are included through the representative list. The families are indexed by the finite choices $(\mathfrak{c}, e, d, \varepsilon)$, with $e^k \mid D(\mathfrak{c})$ and $d \mid B_\Delta$, and by finitely many residue classes from Lemma 2.1. $\square$

Completion of Theorem B. When $r = 0$, the equation is $\kappa z = f(t)$. Retain $f(t) \equiv 0 \pmod{\kappa}$ and set $z = f(t)/\kappa$ using Lemma 2.1; this works for every $f \in \mathbb{Z}[t]$.

Now let $r = 1$ and write the equation as $\kappa x^k y = f(t)$. The split case, including degree at most one, constants and the zero polynomial, was proved in Section 6. For a quadratic $f(t) = At^2 + Bt + C$ irreducible over $\mathbb{Q}$, put

$$\Delta = B^2 - 4AC, \quad T = 2At + B, \quad Y = 4A\kappa y.$$

Then Δ is nonsquare and $T^2 - \Delta = 4Af(t) = x^k Y$. Apply Proposition 7.3, retain the fixed congruences

$$T \equiv B \pmod{2A}, \quad Y \equiv 0 \pmod{4A\kappa},$$

and output $t = (T - B)/(2A)$, $y = Y/(4A\kappa)$ by Lemma 2.1. These substitutions preserve all targets and produce only solutions.

For $k = 1$, [1, Example 7] already expresses the solution set of $xY = T^2 - \Delta$, with $\Delta \neq 0$, as finitely many orbits, each a polynomial family. The same substitutions and fixed congruences give $\kappa xy = f(t)$ in this case. $\square$

8 Five equations: complete solution formulas

The following five equations appear among the open cases in [8, Table 2.3 and Open Question 2.29] and [9, Table 1]. The companion list records that their solution sets are finite unions of polynomial families [10, Sections 8.6 and 8.9]. We give compact formulas and prove that they attain every solution. The first two examples use Theorem A, and the other three use Theorem B. Throughout this section, n is an unrestricted integer parameter.

8.1 Two polynomial parametrizations

The formulas use the following polynomial parametrizations.

- (a) A matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $ad - bc = 1$ may be taken from Vaserstein's published parametrization [1, Theorem 1]. Fixed congruences on its entries are handled by Lemma 2.1.
- (b) Write

$$(a_1, \dots, a_p; b_1, \dots, b_q; R, S) = \mathcal{B}_{p,q}(\theta), \quad \left(\prod_i a_i\right)R + \left(\prod_j b_j\right)S = 1,$$

for the polynomial map, together with its polynomial Bézout coefficients, constructed in Proposition 4.7. Its coordinate tuples cover exactly those with coprime block products. All entries, including R, S , are polynomial outputs on unrestricted integer parameters θ .

Composing the formulas below with these parametrizations and applying Lemma 2.1 gives integer polynomials on unrestricted parameters. Any displayed denominator is the fixed integer 1 or 2, and the displayed congruences are resolved by finite residue subdivision. The proofs establish completeness, including zero coordinates. Using these two parametrizations keeps the displayed formulas short. The total parameter counts are larger: with the unoptimized 150-parameter map of Lemma 3.8, each insertion adds 151 parameters. Filling the first block freely and then the second uses at most $p + q + 151pq$ parameters for $\mathcal{B}_{p,q}$. Thus (8.2) and (8.5) use at most 306 and 609 parameters per residue branch, respectively; the other three formulas use at most 47. These upper bounds come directly from the construction.

8.2 The equation $x^2y + zt + 1 = 0$

For $ad - bc = 1$, all solutions are

$$(x, y, z, t) = (a, -d^2 + bn, b, c(2 + bc) - a^2n). \quad (8.1)$$

Indeed, $a^2d^2 - bc(2 + bc) = (ad - bc)(ad + bc) - 2bc = 1$. Conversely, every solution has $\gcd(x, z) = 1$, so choose a determinant-one completion with $(a, b) = (x, z)$. The displayed particular solution and the kernel vector $(b, -a^2)$ give every pair (y, t) . This remains valid when $a = 0$ or $b = 0$.

8.3 The equation $x_1x_2x_3 + x_4x_5 + 1 = 0$

Take $(a, b; c; R, S) = \mathcal{B}_{2,1}(\theta)$. Then all solutions are

$$(x_1, x_2, x_3, x_4, x_5) = (a, b, -R + cn, c, -S - abn). \quad (8.2)$$

The identity follows from $abR + cS = 1$. Conversely, the equation forces $\gcd(x_1x_2, x_4) = 1$, so the map $\mathcal{B}_{2,1}$ attains $(a, b, c) = (x_1, x_2, x_4)$. For any supplied Bézout coefficients R, S , the kernel vector $(c, -ab)$ gives every pair (x_3, x_5) , including all zero cases.

8.4 The equation $x^2y + z^2 - 1 = 0$

For $ad - bc = 1$, put

$$R = d^2(1 - 2bc), \quad S = c^2(1 + 2ad), \quad a^2R + b^2S = 1.$$

For either $\eta = 1$ or $\eta = 2$, all the following triples are solutions, and together the two formulas cover every solution:

$$\boxed{\begin{aligned} x &= \eta ab, \\ y &= ((2/\eta)R + b^2n)((2/\eta)S - a^2n), \\ z &= a^2R - b^2S + \eta a^2b^2n. \end{aligned}} \quad (8.3)$$

Here $2/\eta$ is the fixed integer 2 or 1. The factors of $1 - z^2$ are

$$z + 1 = a^2(2R + \eta b^2n), \quad 1 - z = b^2(2S - \eta a^2n),$$

which prove the equation.

For completeness, if x is odd, allocate its prime powers between $z + 1$ and $z - 1$, whose gcd divides 2. This gives $x = ab$, $\gcd(a, b) = 1$, $a^2 \mid z + 1$, and $b^2 \mid z - 1$. If $z = \pm 1$, allocate all prime powers to the vanishing factor. Choose c, d completing (a, b) ; the Chinese remainder theorem gives $z = a^2R - b^2S + a^2b^2n$, the $\eta = 1$ formula. If $x \neq 0$ is even, then z is odd and $(z + 1)/2, (z - 1)/2$ are coprime. Allocating the prime powers of $x/2$ gives $x = 2ab$, $a^2 \mid (z + 1)/2$, and $b^2 \mid (z - 1)/2$. Put $z_0 = a^2R - b^2S$. Since $z_0 + 1 = 2a^2R$ and $1 - z_0 = 2b^2S$, both $2a^2$ and $2b^2$ divide $z - z_0$. Their least common multiple is $2a^2b^2$, giving the $\eta = 2$ formula. In both cases the equation determines y as displayed. Finally, for $x = 0$, the $\eta = 2$ formula with $(a, b) = (0, 1)$ or $(1, 0)$ gives $z = -1$ or 1 , respectively, and lets y range over all integers.

8.5 The equation $x^2y + z^2 + 1 = 0$

Take $ad - bc = 1$ with the fixed parity conditions $c \equiv d \equiv 1 \pmod{2}$, and set

$$A = a^2 + b^2, \quad U = ac + bd, \quad V = c^2 + d^2, \quad H = UV/2 + An.$$

Together, the choices $\varepsilon = 1$ and $\varepsilon = -1$ cover all solutions:

$$\boxed{(x, y, z) = (\varepsilon A, -V^2 - 2Un - H^2, U + AH).} \quad (8.4)$$

The denominator 2 is fixed and V is even. Since $AV - U^2 = (ad - bc)^2 = 1$, direct expansion gives

$$(U + AH)^2 + 1 = A^2(V^2 + 2Un + H^2).$$

For completeness, every solution has $x \neq 0$ and $A = |x|$ odd. Unique factorization in $\mathbb{Z}[i]$ supplies a Gaussian divisor $a + bi$ of $z - i$ with norm A and $\gcd(a, b) = 1$: each odd prime $p \mid A$ splits, and its two conjugate Gaussian prime factors cannot both divide $z - i$, whose imaginary part is -1 . For the unique factor π dividing $z - i$, $v_\pi(z - i) = v_p(z^2 + 1) \geq 2v_p(A)$. Taking the factor $\pi^{v_p(A)}$ for each $p \mid A$ gives the required divisor. Write

$$z - i = (a + bi)(c_0 - d_0i).$$

Then $ad_0 - bc_0 = 1$ and $ac_0 + bd_0 = z$. The integers a, b have opposite parity. Replacing (c_0, d_0) by $(c_0 + a\tau, d_0 + b\tau)$ for a suitable integer τ makes both entries odd and preserves the determinant, while making $U \equiv z \pmod{A}$. At $n = 0$, the displayed formula gives a root Z_0 of $Z_0^2 + 1 \equiv 0 \pmod{A^2}$ with $Z_0 \equiv z \pmod{A}$. Since $\gcd(2z, A) = 1$, this root lifts uniquely from modulo A to modulo A^2 : from $A^2 \mid (Z_0 - z)(Z_0 + z)$ one obtains $A^2 \mid Z_0 - z$. Varying n changes z by A^2n , so every target z is attained. The sign ε gives the prescribed x , and the original equation then fixes y .

8.6 The equation $xyz + t^2 - 1 = 0$

Take $(a, c; b, d; R, S) = \mathcal{B}_{2,2}(\theta)$ and put

$$P = ac, \quad Q = bd, \quad U = 2R + Qn, \quad V = 2S - Pn.$$

For each $(h, k) \in \{(1, 1), (2, 1), (1, 2)\}$, retain the fixed congruence $UV \equiv 0 \pmod{hk}$ and set

$$(x, y, z, t) = (hab, kcd, UV/(hk), PR - QS + PQn). \quad (8.5)$$

Add the six linear families obtained by setting $t = \pm 1$ and one of x, y, z equal to zero, leaving the other two free. Together these families cover all solutions. Indeed, $PR + QS = 1$ gives $t + 1 = PU$ and $1 - t = QV$, so $1 - t^2 = PQUV = xyz$. The denominator hk is the fixed integer 1 or 2.

For completeness when $t \neq \pm 1$, the three coordinates x, y, z are nonzero. All odd prime powers of xy can be allocated wholly to $t + 1$ or $t - 1$. At 2, at most one of $t + 1, t - 1$ has valuation greater than 1. If xy is even, remove one factor 2 from an even coordinate of x, y , choosing $(h, k) = (2, 1)$ or $(1, 2)$; otherwise choose $(1, 1)$. The remaining 2-valuation of $xy/(hk)$ fits in one root factor. Thus one can factor $x/h = ab$, $y/k = cd$ with $\gcd(ac, bd) = 1$, $ac \mid t + 1$, and $bd \mid t - 1$. The map $\mathcal{B}_{2,2}$ attains these coordinates. For its supplied Bézout coefficients R, S , the Chinese remainder theorem gives $t = PR - QS + PQn$. The target equation then gives $UV = hkz$, including the required fixed congruence. The six linear families cover $t = \pm 1$.

Use of AI. OpenAI's ChatGPT and Codex assisted in developing the arguments, checking identities, and drafting and revising this manuscript. A review generated by Anthropic's Claude Opus 5.5 informed the revision.

References

- [1] L. N. Vaserstein, *Polynomial parametrization for the solutions of Diophantine equations and arithmetic groups*, Ann. of Math. (2) **171** (2010), no. 2, 979–1009. <https://doi.org/10.4007/annals.2010.171.979>.
- [2] S. Frisch, *Remarks on polynomial parametrization of sets of integer points*, Comm. Algebra **36** (2008), no. 3, 1110–1114. <https://doi.org/10.1080/00927870701776938>.
- [3] S. Frisch and G. Lettl, *Polynomial parametrization of the solutions of Diophantine equations of genus 0*, Funct. Approx. Comment. Math. **39** (2008), no. 2, 205–209. <https://doi.org/10.7169/facm/1229696571>.
- [4] W. Bruns, J. Gubeladze and N. V. Trung, *Problems and algorithms for affine semigroups*, Semigroup Forum **64** (2002), 180–212. <https://doi.org/10.1007/s002330010099>.
- [5] D. Cox, J. Little and D. O’Shea, *Using Algebraic Geometry*, Graduate Texts in Mathematics 185, Springer, 1998. <https://doi.org/10.1007/978-1-4757-6911-1>.
- [6] A. V. Sutherland, *Properties of Dedekind domains*, MIT 18.785, Lecture 3, Fall 2017, Corollary 3.20. <https://math.mit.edu/classes/18.785/2017fa/LectureNotes3.pdf>.
- [7] A. V. Sutherland, *The Minkowski bound and finiteness results*, MIT 18.785, Lecture 14, Fall 2017. <https://math.mit.edu/classes/18.785/2017fa/LectureNotes14.pdf>.
- [8] B. Grechuk, *Polynomial Diophantine Equations: A Systematic Approach*, Springer, 2024. <https://doi.org/10.1007/978-3-031-62949-5>.
- [9] B. Grechuk, *A systematic approach to Diophantine equations: open problems*, arXiv:2404.08518v1, 12 April 2024. <https://arxiv.org/abs/2404.08518v1>.
- [10] B. Grechuk, *A systematic approach to Diophantine equations: open problems*, arXiv:2404.08518v10, 1 October 2026. <https://arxiv.org/abs/2404.08518v10>.