

Step counts in integrable rational maps as discrete logarithms: a complete, formally verified theory of orbits on every level

Yuta Ogura
Independent researcher

Version 1 — October 2026

Abstract

For a rational map σ of a finite-dimensional space over a field K and two states s, t , we determine the set $\text{Id}(s, t) = \{n \in \mathbb{Z} : \sigma^n s = t\}$ of step counts—the hom-set from s to t in the action groupoid of the dynamics—without iterating the map. For the Lyness map, the Kahan–Hirota–Kimura discretisation of the Euler top, area-preserving linear maps and a Kahan discretisation of hyperbolic geodesics, we prove, in Lean 4 with Mathlib and for every field (characteristic $\neq 2$ where needed), that on every level set of the conserved quantities the map is a translation by a fixed element P of an abelian group A attached to the level, along an injective coordinate ψ . Hence $\sigma^n s = t$ if and only if $\psi(t) - \psi(s) = nP$. Step counts are discrete logarithms, $\text{Id}(s, t)$ is empty or a residue class modulo the order of P , and the class of $\psi(s)$ modulo $\langle P \rangle$ is a complete invariant of the orbits. The theorems also cover the degenerate levels (nodal and reducible curves, and the levels of the Euler top with vanishing coordinates). Two further results make the theory usable as a decision procedure. First, the states at which the map is undefined are finitely many explicit states of each level, so whether an orbit ever meets a division by zero (that is, whether the state is *regular*) is decided by a few more discrete logarithms, in both time directions, and a non-regular state’s finite chain is read off the same logarithms. Second, a reduction theorem for partial rational maps lifts regularity and the absence of paths from the reductions modulo primes to $\mathbb{Q}$ and reduces step counts from $\mathbb{Q}$ modulo primes, so that, given a bound on $|n|$, questions over $\mathbb{Q}$, including the negative answer “never”, are settled by finitely many primes and one exact iteration. The dynamics is also axiomatised as a small Martin-Löf theory with a path constant $\text{path} : \Pi x. \text{Id}(x, \text{step } x)$ and interpreted in the groupoid model of HoTTLean, where the identity type between s and t is exactly the set $\text{Id}(s, t)$. The development comprises 1,146 theorems with no `sorry` and only the standard axioms, and includes an executable certificate checker whose soundness is itself proved in Lean. It is the mathematical foundation of Structure Computer, which answers these questions with independently checkable certificates: on a 2-core machine, a state 7.9×10^{15} steps away over $\mathbb{F}_{2^{61}-1}$ is located in 0.4 s, where iteration would take about a century.

Contents

1	Introduction	2
1.1	The question	2
1.2	Integrable maps as translations	3
1.3	Contributions	3

2	The setting	4
2.1	Partial flows and regular states	4
2.2	The three answers	4
2.3	The action groupoid	5
3	Phases: translation flows on groups	5
4	The Lyness map	5
4.1	The map and its integral	5
4.2	Elliptic levels	6
4.3	Nodal levels	6
4.4	The reducible levels $k = 0$ and $k = a - 1$	6
5	The Kahan–Hirota–Kimura discretisation of the Euler top	7
5.1	The step and the integrals	7
5.2	The universal top and its levels	8
5.3	Elliptic levels	8
5.4	Every level: cases A, B, Z	8
6	Linear flows, the discretised oscillator and E2	9
7	Regularity by the phase	9
8	Reduction to the rationals	10
9	The type-theoretic content	11
10	The formalisation	11
10.1	Scope and statistics	11
10.2	Proof technique	12
10.3	Non-vacuity	12
10.4	A certificate checker proved sound	12
11	Related work	12
12	Scope and further work	13
A	Worked examples	13

1 Introduction

1.1 The question

A discrete dynamical system is a state space X with a map $\sigma : X \rightarrow X$, the step. Given two states s and t , after how many steps—if ever—is t reached from s ? When σ is invertible the complete answer is the set

$$\text{Id}(s, t) = \{ n \in \mathbb{Z} : \sigma^n s = t \},$$

which is empty or a coset $r + M\mathbb{Z}$, where $M \geq 0$ is the period of the orbit ($M = 0$ for an infinite orbit). The notation is the type-theoretic one: $\text{Id}(s, t)$ is the hom-set from s to t in the action groupoid $X//\mathbb{Z}$, and Section 9 makes the connection exact.

When σ is a rational map over $\mathbb{F}_q$ with $q \approx 2^{61}$, a typical orbit has about q states and cannot be followed; and “ t is never reached” can be established only by following the whole

orbit. Over $\mathbb{Q}$ orbits are in general infinite, and iteration never settles a negative answer. One needs a description of the orbit from which membership and step counts can be read off directly.

1.2 Integrable maps as translations

For integrable maps such a description is available: the map acts as a translation on each level curve. A planar map of QRT type [23, 24] preserves a pencil of biquadratic curves and acts on each smooth member—an elliptic curve—as a translation by a fixed element of its group [8]. The Lyness map $(x, y) \mapsto (y, (a + y)/x)$ is the simplest example; its level curves $(x + 1)(y + 1)(x + y + a) = kxy$ govern its real dynamics [3], and Hone [10, 11] used the translation structure over $\mathbb{Z}/N$ for elliptic-curve factorisation. The Kahan–Hirota–Kimura discretisation of the Euler top [9, 13] is integrable, with two independent rational integrals [4, 19, 20], and its level curves are elliptic as well. Once a level is identified with a group A on which the step is translation by P , the question $\text{Id}(s, t)$ is a discrete logarithm, computable over a finite field by Pohlig–Hellman [21] in time about the square root of the largest prime factor of the group order; for linear maps this is the orbit problem of Kannan and Lipton [6, 14], and for elliptic divisibility sequences the identification of index recovery with the elliptic discrete logarithm problem is due to Lauter and Stange [15].

1.3 Contributions

This paper turns the translation structure into a decision procedure for the four families, and formalises it.

- (i) **Every level, every field (Sections 4–6).** For the four families we identify, on every level set, the group A , the translation point P and the coordinate ψ , and prove the translation theorem together with the exact region on which ψ is injective. This includes the levels where the curve is nodal or splits into lines and conics (with eigen-coordinates in a quadratic extension when the relevant discriminant is a non-square, and additive coordinates in the parabolic cases), the levels of the Euler top with one or two vanishing coordinates, and the fixed points and equilibria. The statements are proved over an arbitrary field (of characteristic $\neq 2$ where needed), with Mathlib’s Weierstrass curves and their group law [1, 26] as the foundation.
- (ii) **Regularity by the phase (Section 7).** A rational map is undefined on its singular set. We show that on each level the states at which the step or its inverse is undefined are explicit and few: at most two for the Lyness map, and for the Euler top at most 56 candidates, obtained from the roots of two polynomials of degree at most 3 and 4 in the multiplier of the level; a state is regular if and only if no stuck state lies in its coset $\psi(s) + \langle P \rangle$. Regularity is thereby decided without iteration, in both time directions, and for a non-regular state the same logarithms give its finite chain and the unique step count to t on it, if any.
- (iii) **Reduction to $\mathbb{Q}$ (Section 8).** For rational data we prove that regularity modulo a prime pulls back to $\mathbb{Q}$, that step counts over $\mathbb{Q}$ reduce modulo p , and that the absence of a path modulo p lifts to $\mathbb{Q}$. With the Chinese remainder theorem over a few primes and one exact rational iteration this decides $\text{Id}(s, t)$ over $\mathbb{Q}$, and in particular returns the unconditional answer “never”, which no iteration can give.
- (iv) **The type-theoretic content (Section 9).** The dynamics is a theory with five constants in Martin–Löf type theory, interpreted in the groupoid model of HoTTLean [17]; the

identity type between the closed terms s and t is interpreted by $\text{Id}(s, t)$, the loop space by the period subgroup, and the soundness of the interpretation yields that no identity between states on different orbits is derivable.

- (v) **A verified checker (Section 10.4).** Beyond the theorems, the development contains an executable checker for the certificates of the Lyness map over $\mathbb{F}_q$, written in core Lean, with a soundness theorem: whatever it accepts is true of the Lean definitions.

Everything is formalised: 1,146 theorems in Lean 4 [7], no sorry, only the axioms `propext`, `Classical.choice` and `Quot.sound`, and every principal theorem instantiated at concrete states with all hypotheses discharged inside Lean, so that none is vacuous (Section 10.3). The theory is the foundation of Structure Computer [18], a system that answers $\text{Id}(s, t)$ and related structural questions with certificates an independent checker verifies. To give one example: for the Lyness map with $a = 3$ over $\mathbb{F}_q$, $q = 2^{61} - 1$, the state $t = (813066766938016773, 992646061924517494)$ is reached from $s = (2, 5)$ exactly at $n \equiv 7,863,588,611,074,867 \pmod{576,460,752,629,115,698}$, computed and checked in 0.4 s, where iterating the map at the measured 2.6×10^6 steps per second would take about 96 years (Appendix A).

2 The setting

2.1 Partial flows and regular states

A rational map is not everywhere defined: the Lyness step is undefined where $x = 0$ or $a + y = 0$, and its inverse where $y = 0$ or $a + x = 0$. We therefore work with *partial flows*.

Definition 2.1 (partial flow). A partial flow on a set S is a pair of partial maps $f, g : S \rightharpoonup S$ that are mutually inverse where defined: $f(x) = y$ implies $g(y) = x$ and conversely.

Definition 2.2 (regular state). A state s is *regular* if every forward iterate $f^n(s)$ and every backward iterate $g^n(s)$, $n \in \mathbb{N}$, is defined.

The regular states are closed under f and g , and f restricts to a permutation σ of them, with inverse g ; we call this the *regular flow* and write σ^n for its integer powers. On a finite state space, regular is the same as periodic, so for small q regularity is cycle detection; Section 7 decides it without iterating. A non-regular state lies on a finite *chain*: iterating f from it stops at a *forward-stuck* state where f is undefined, and iterating g stops at a backward-stuck state. A target is reached from a chain at most once.

2.2 The three answers

For states s, t , the question $\text{Id}(s, t)$ has exactly one of three answers:

- **steps** (r, M) : s and t are regular and $\{n : \sigma^n s = t\} = r + M\mathbb{Z}$ with $M \geq 0$ (over $\mathbb{Q}$ the answer is given relative to a bound on $|n|$);
- **no path**: s is regular and $\sigma^n s \neq t$ for every $n \in \mathbb{Z}$ (including the case that t is not regular);
- **not regular**: s is not regular; the answer gives the length of its forward chain and the at most one n with $f^n s = t$ ($n \geq 0$) or $g^{-n} s = t$ ($n < 0$).

2.3 The action groupoid

A flow (S, σ) is a $\mathbb{Z}$ -set, and its *action groupoid* $S//\mathbb{Z}$ has the states as objects and the integers n with $\sigma^n s = t$ as morphisms from s to t . The hom-set $\text{Hom}(s, t) = \text{Id}(s, t)$ is our object of study; the automorphism group of s is the period subgroup $M\mathbb{Z}$, the fundamental group of the orbit.

3 Phases: translation flows on groups

Definition 3.1 (phase). Let $\Phi = (S, \sigma)$ be a flow, A an abelian group, $P \in A$, $\psi : S \rightarrow A$, and $R \subseteq S$ a region with $R(\sigma x) \iff R(x)$. The pair (ψ, P) is a *phase* on R if $\psi(\sigma x) = \psi(x) + P$ for all $x \in R$ and ψ is injective on R .

Theorem 3.2 (translation flows). Let (ψ, P) be a phase on R and $s, t \in R$. For every $n \in \mathbb{Z}$,

$$\sigma^n s = t \iff \psi(t) - \psi(s) = nP.$$

Hence $\text{Id}(s, t) = \{n \in \mathbb{Z} : \psi(t) - \psi(s) = nP\}$, which is empty if $\psi(t) - \psi(s) \notin \langle P \rangle$ and otherwise a residue class modulo the order of P ; and s, t lie on one orbit if and only if $\psi(s) \equiv \psi(t) \pmod{\langle P \rangle}$.

Proof. Induction gives $\psi(\sigma^n x) = \psi(x) + nP$ for $n \in \mathbb{Z}$ and $x \in R$, using the invariance of R in both directions. If $\sigma^n s = t$ then $\psi(t) = \psi(s) + nP$. Conversely if $\psi(t) = \psi(\sigma^n s)$, then $t = \sigma^n s$ by injectivity on R . Uniqueness of n modulo the order of P is the definition of the order. $\square$

The class of $\psi(x)$ in $A/\langle P \rangle$ is the *phase* of x ; it is conserved and, by the theorem, complete: the phase refines the level by $A/\langle P \rangle$; over a finite field the number of orbits on the level is at most $|A/\langle P \rangle|$. The two states of Example A.7, which share both independent integrals of the Euler top yet lie on different orbits, are separated by their phases.

For a cyclic $A = \langle g \rangle$ with $P = eg$ and $\psi(t) - \psi(s) = jg$, the condition reads $en \equiv j \pmod{\text{ord } g}$, solvable iff $\gcd(e, \text{ord } g) \mid j$; orders and logarithms are computed by Pohlig–Hellman, and the residue class is assembled by the Chinese remainder theorem from the prime-power parts. For a non-cyclic A (an elliptic curve $\mathbb{Z}/n_1 \times \mathbb{Z}/n_2$, or a product with $(\mathbb{Z}/2)^r$) the same holds componentwise, and non-membership $\psi(t) - \psi(s) \notin \langle P \rangle$ is witnessed inside one prime-power component. The development also treats partial translations: for a forbidden set $B \subseteq A$, the partial map $a \mapsto a + P$ (defined when $a, a + P \notin B$) has a regular iff the coset $a + \langle P \rangle$ avoids B —the abstract form of Section 7.

4 The Lyness map

Throughout, K is a field and $a \in K$.

4.1 The map and its integral

The Lyness map with parameter a is the partial flow

$$T(x, y) = \left(y, \frac{a+y}{x}\right) (x \neq 0, a+y \neq 0), \quad T^{-1}(x, y) = \left(\frac{a+x}{y}, x\right) (y \neq 0, a+x \neq 0),$$

the first-order form of $x_{n+1}x_{n-1} = a + x_n$; the condition $a+y \neq 0$ is what makes T^{-1} defined at the image. Its integral is

$$I(x, y) = \frac{(x+1)(y+1)(x+y+a)}{xy},$$

and $I(Tx) = I(x)$ wherever T is defined. A state is on the level k when $xy \neq 0$ and $kxy = (x+1)(y+1)(x+y+a)$; states on different levels are never joined.

4.2 Elliptic levels

For a level k let $W_k : Y^2 = X^3 + A_2X^2 + A_4X + A_6$ with

$$A_2 = (a - k)^2 - 4a + 2k + 4, \quad A_4 = 4k((a - k)^2 - 2a + k), \quad A_6 = 4k^2((a - k)^2 + 2k),$$

a Weierstrass curve with discriminant $\Delta(W_k) = 4096k^3(a - k - 1)^2(a^3 - 2a^2k - 6a^2 + ak^2 - 10ak + 12a + k - 8)$; the level is *elliptic* when $\Delta \neq 0$, which forces $k \neq 0$, $k \neq a - 1$ and $\text{char } K \neq 2$. Put

$$U = -2(k + 2xy + 2x + 2y + 2), \quad V = -4(a(x + 1)(y + 1) - k(xy + x - y) + 2y(x + 1)(y + 1)),$$

$$\varphi(x, y) = (U, V), \text{ and } Q = (2k, 4k(a - k - 1)).$$

Theorem 4.1 (elliptic levels). *If $\Delta(W_k) \neq 0$, then φ maps the level k into $W_k(K)$, $Q \in W_k(K)$, $\varphi(T(x, y)) = \varphi(x, y) + Q$ in the group law of W_k whenever $T(x, y)$ is defined, and φ is injective on the level. Consequently, for regular states s, t of the level and all $n \in \mathbb{Z}$,*

$$T^n s = t \iff \varphi(t) - \varphi(s) = nQ,$$

and the class of $\varphi(s)$ in $W_k(K)/\langle Q \rangle$ is a complete invariant of the orbits on the level.

The first three statements reduce to polynomial identities conditional on the level equation, proved against Mathlib's addition formulas. Over $\mathbb{F}_q$ the computation of $\text{Id}(s, t)$ is thus an elliptic-curve discrete logarithm in a group of order about q ; for $q = 2^{61} - 1$ it takes well under a second whenever that order has no prime factor above roughly 2^{40} (Example A.2, with a factor near 2^{45} , takes 18 s).

4.3 Nodal levels

When $\Delta(W_k) = 0$ but $k \neq 0$, $k \neq a - 1$ and $2 \neq 0$, the cubic W_k has exactly one singular point, and its nonsingular points form a group with the same addition formulas. Call a state *good* if it is on the level and $\varphi(x, y)$ is a nonsingular point of W_k .

Theorem 4.2 (nodal levels). *Under these hypotheses the good states form an invariant region on which $\varphi \circ T = \varphi + Q$ and φ is injective, so Theorem 3.2 holds on the good states with the group of nonsingular points of W_k ; a state of the level that is not good is a fixed point of T .*

4.4 The reducible levels $k = 0$ and $k = a - 1$

On the two levels excluded by the discriminant the curve is reducible, T permutes its components, and a power of T acts on each component as a Möbius transformation; the group is the multiplicative or additive group of an eigen-coordinate extended by a finite cyclic group recording the component.

$k = 0$: three lines. The level is $x = -1$, $x + y + a = 0$, $y = -1$, cycled by T . On $x = -1$ the map T^3 has fixed points $y = 1 - a$ and $y = -1$ and multiplies $\ell = (y + 1)/(y + a - 1)$ by $(a - 1)^{-1}$. Off the vertices $(x, y \neq 1 - a, (x, y) \neq (-1, -1))$ define v , from the level to $K^\times \times \mathbb{Z}$, by $(\frac{y+1}{y+a-1}, 0)$ on $x = -1$, $(\frac{x+a-1}{x+1}, 2)$ on $y = -1$, and $(\frac{x+1}{x+a-1}, 1)$ otherwise.

Theorem 4.3. *For $a \neq 1, 2$, the class $\psi = [v]$ in $G = (K^\times \times \mathbb{Z})/\langle((a - 1)^{-1}, -3)\rangle$ satisfies $\psi(Tx) = \psi(x) + [(1, 1)]$ and is injective off the vertices; Theorem 3.2 holds there with $A = G$, $P = [(1, 1)]$.*

Over $\mathbb{F}_q$ the group has order $3(q - 1)$; the vertices form orbits of length at most 3. For $a = 2$ the three lines are concurrent and the Möbius map is parabolic; the coordinate $c = 1/(y + 1)$ is additive and the group is $(K \times \mathbb{Z})/\langle(1, -3)\rangle$, of order $3q$ over $\mathbb{F}_q$.

$k = a - 1$: **a line and a conic.** Since $(x + 1)(y + 1)(x + y + a) - (a - 1)xy = (x + y + 1)((x + 1)(y + 1) + a - 1)$, the level is the line $x + y + 1 = 0$ and the conic $(x + 1)(y + 1) = 1 - a$, swapped by T . On the line T^2 is $z \mapsto (a - 1 - z)/z$ with fixed points x_1, x_2 , the roots of $z^2 + z + 1 - a$; with $\ell(z) = (z - x_1)/(z - x_2)$, T^2 multiplies ℓ by x_2/x_1 . The eigen-coordinate lives in $L = K(x_1, x_2)$.

Theorem 4.4. *Let $L \supseteq K$ contain $x_1 \neq x_2$ with $x_1 + x_2 = -1$, $x_1 x_2 = 1 - a$, and $a \neq 1$. On the states of the level with $x \neq x_1, x_2$, the map ψ to $(L^\times \times \mathbb{Z})/\langle(x_2/x_1, -2)\rangle$ given by $[(\ell(x), 0)]$ on the line and $[(\ell(-1 - x), 1)]$ on the conic is a phase with $P = [(1, 1)]$. If moreover $2 \neq 0$ and $4a - 3$ is not a square in K , then with $L = K(\sqrt{4a - 3})$ no state is excluded: the phase is complete on the whole level.*

Over $\mathbb{F}_q$ the phase takes values in a subgroup of order $2(q - 1)$ (split) or, in the norm-one part of $L^\times$, $2(q + 1)$ (non-split). The tangent case $4a = 3$ is parabolic with group $(K \times \mathbb{Z})/\langle(-2, -2)\rangle$, and for $a = 1$, where the two reducible levels coincide, every orbit has period 5 and $\text{Id}(s, t)$ is read off five steps. Table 1 summarises the levels; the nodal and parabolic cases require $\text{char } K \neq 2$.

level	condition	group A	P
elliptic	$\Delta(W_k) \neq 0$	$W_k(K)$	$(2k, 4k(a - k - 1))$
nodal	$k \neq 0, a - 1; 2 \neq 0; \Delta = 0$	nonsingular points of W_k	same
$k = 0$	$a \neq 1, 2$	$(K^\times \times \mathbb{Z})/\langle((a - 1)^{-1}, -3)\rangle$	$[(1, 1)]$
$k = 0, a = 2$		$(K \times \mathbb{Z})/\langle(1, -3)\rangle$	$[(0, 1)]$
$k = a - 1$	$a \neq 1; x_1 \neq x_2 \text{ in } L$	$(L^\times \times \mathbb{Z})/\langle(x_2/x_1, -2)\rangle$	$[(1, 1)]$
$k = a - 1, 4a = 3$		$(K \times \mathbb{Z})/\langle(-2, -2)\rangle$	$[(0, 1)]$

Table 1: The levels of the Lyness map and their phases.

5 The Kahan–Hirota–Kimura discretisation of the Euler top

Throughout, $\text{char } K \neq 2$ and $h a_1 a_2 a_3 \neq 0$.

5.1 The step and the integrals

The Euler top is $\dot{x}_1 = a_1 x_2 x_3$, $\dot{x}_2 = a_2 x_3 x_1$, $\dot{x}_3 = a_3 x_1 x_2$. Its Kahan discretisation [4, 13], which coincides with that of Hirota and Kimura [9], replaces each product by its polarisation:

$$\tilde{x} - x = h B(x, \tilde{x}), \quad B(x, y) = (a_1(x_2 y_3 + x_3 y_2), a_2(x_3 y_1 + x_1 y_3), a_3(x_1 y_2 + x_2 y_1)),$$

with h equal to Hirota and Kimura's ϵ . The equation is linear in $\tilde{x}$, $(1 - hJ(x))\tilde{x} = x$ with $J(x)\tilde{x} = B(x, \tilde{x})$, with determinant $D_h(x) = 1 - h^2(a_2 a_3 x_1^2 + a_3 a_1 x_2^2 + a_1 a_2 x_3^2) - 2h^3 a_1 a_2 a_3 x_1 x_2 x_3$, so the step is the rational map $T_h(x) = \text{adj}(1 - hJ(x))x/D_h(x)$, reversible with $T_h^{-1} = T_{-h}$. The three Hirota–Kimura integrals are

$$I_{12} = \frac{a_2 x_1^2 - a_1 x_2^2}{1 - h^2 a_1 a_2 x_3^2}, \quad I_{23} = \frac{a_3 x_2^2 - a_2 x_3^2}{1 - h^2 a_2 a_3 x_1^2}, \quad I_{31} = \frac{a_1 x_3^2 - a_3 x_1^2}{1 - h^2 a_3 a_1 x_2^2};$$

along a defined step every numerator and every denominator is multiplied by one common factor, so the three ratios are conserved; two of them are independent.

5.2 The universal top and its levels

The rescaling $u_i = \lambda_i x_i$ with $\lambda_1^2 = h^2 a_2 a_3$, $\lambda_3^2 = h^2 a_1 a_2$, $\lambda_1 \lambda_3 = h a_2 \lambda_2$ (such λ_i exist in a tower of two quadratic extensions $L \supseteq K$) conjugates every top to the *universal top* $a = (1, 1, 1)$, $h = 1$. There, with $D(u) = 1 - u_1^2 - u_2^2 - u_3^2 - 2u_1 u_2 u_3$ and $y(u) = (1 - u_1^2, 1 - u_2^2, 1 - u_3^2)$, the vector y is multiplied by a scalar along each step, so the *level* of a state is the point $\alpha = [y(u)] \in \mathbb{P}^2(K)$, defined when $y(u) \neq 0$; the case $y(u) = 0$ is the base level of Section 5.4.

5.3 Elliptic levels

Fix a representative $(\alpha_1, \alpha_2, \alpha_3)$ of α , let c_1, c_2, c_3 be its elementary symmetric functions, and let

$$W_\alpha : Y^2 - 2c_1 XY - 4c_3 Y = X^3 - (c_1^2 - c_2)X^2 - 3c_1 c_3 X - 3c_3^2,$$

with discriminant $16(\alpha_1 \alpha_2 \alpha_3)^2 \prod_{i < j} (\alpha_i - \alpha_j)^2$: the level is elliptic exactly when the α_i are nonzero and distinct. For u on the level write $y(u) = m\alpha$ (m is the *multiplier* of u) and put $\varphi_\alpha(u) = (N(u)/m^2, R(u)/m^3)$, where, with $\pi = (1 + u_1)(1 + u_2)(1 + u_3)$,

$$N = \pi(u_1 + u_2 + u_3 - 1), \quad R = -\pi \left(\sum_i (u_i^3 - u_i^2 - u_i) - 2(u_1 u_2 + u_1 u_3 + u_2 u_3) + 1 \right),$$

and let $Q = (0, c_3)$.

Theorem 5.1 (elliptic levels of the top). *If $\Delta(W_\alpha) \neq 0$, then φ_α maps the level into $W_\alpha(K)$, $Q \in W_\alpha(K)$, $\varphi_\alpha(Tu) = \varphi_\alpha(u) + Q$ whenever Tu is defined, and φ_α has an explicit rational inverse on the states that take two defined steps. Hence Theorem 3.2 holds for the universal top on the regular states of the level and, through the rescaling, for every top, the phase then taking values in a curve over the extension L .*

The identities are unconditional polynomial identities in u of degree up to 12.

5.4 Every level: cases A, B, Z

Every level of the universal top falls, after a cyclic permutation of the coordinates, into one of three cases, or is vacuous.

Case A: all $\alpha_i \neq 0$. W_α may be nodal or cuspidal when two α_i coincide; $\varphi_\alpha(u)$ is nonsingular exactly when the pairwise sums $u_i + u_j$ are nonzero, since both partial derivatives of the equation of W_α at $\varphi_\alpha(u)$ are multiples of $\pi(u_1 + u_2)(u_1 + u_3)(u_2 + u_3)$; the Y -derivative $2Y - 2c_1 X - 4c_3$, for instance, equals $2\pi(u_1 + u_2)(u_1 + u_3)(u_2 + u_3)/m^3$. The even sign changes form a group $V \cong (\mathbb{Z}/2)^2$ commuting with the step; among the four images gu , $g \in V$, one has a nonsingular φ_α -image unless two coordinates of u vanish. The phase is $(\varphi_\alpha(g_u u), g_u) \in W_\alpha^{\text{ns}} \times V$, where g_u is the selected element, and $P = (Q, 0)$.

Case B: $\alpha_3 = 0$, $\alpha_1 \neq \alpha_2$ **nonzero**. Then $u_3 = \pm 1$, the step swaps the components $u_3 = 1$ and $u_3 = -1$ of the level, and φ_α , applied after mapping $u_3 = -1$ to $u_3 = 1$, is translated by $P' = (\alpha_2(\alpha_2 - \alpha_1), \alpha_2(\alpha_2 - \alpha_1)(2\alpha_2 + \alpha_1))$; the phase is in $W_\alpha^{\text{ns}} \times \mathbb{Z}/2$ with $P = (P', 1)$.

Case Z: $\alpha_2 = \alpha_3 = 0$. Here $u_2, u_3 = \pm 1$ and the step is $(u_1, u_2, u_3) \mapsto (u_1 - 2u_2 u_3, -u_2, -u_3)$; writing $[\pm 1] \in \mathbb{Z}/2$ for the sign class, the phase is $(u_1 u_2 u_3, [u_2], [u_2 u_3]) \in K \times (\mathbb{Z}/2)^2$ with $P = (-2, 1, 0)$.

Levels without regular states. On $\alpha = (c, c, 0)$ and at states with $y(u) = 0$ no state takes two consecutive steps, so there are no regular states; equilibria (two zero coordinates) are fixed points.

Theorem 5.2 (every level of every top). *Let $\text{char } K \neq 2$, $ha_1a_2a_3 \neq 0$, and fix a level. There are an abelian group A , $P \in A$ and a map ψ on the regular states such that for all regular non-equilibrium states s, t on that level: $\sigma^n s = t \iff \psi(t) - \psi(s) = nP$ for every $n \in \mathbb{Z}$; s, t lie on one orbit iff $\psi(t) - \psi(s) \in \langle P \rangle$; and if $\psi(t) - \psi(s) \notin \langle P \rangle$ no identity between s and t is derivable in the sense of Section 9.*

Remark 5.3. The extension L cannot in general be avoided: when $h^2a_2a_3$ is a non-square the phase of an $\mathbb{F}_q$ -rational state lies in $W_\alpha(\mathbb{F}_{q^2})$, a group of order $\approx q^2$. Finding the order of a point there by baby-step giant-step in the Hasse interval costs about $q^{1/2}$ operations, against $q^{1/4}$ for a curve over $\mathbb{F}_q$, which is why in practice the Euler top reaches $q \approx 2^{45}$ and the Lyness map 2^{61} .

6 Linear flows, the discretised oscillator and E2

The oscillator. The discretised harmonic oscillator $\sigma(x, y) = (y, -x + 2cy)$ has the integral $x^2 + y^2 - 2cxy$. If $l \in L^\times$ satisfies $l + l^{-1} = 2c$, $l \neq l^{-1}$, the eigen-coordinates $x - ly$ and $x - l^{-1}y$ are multiplied by $l^{\pm 1}$ and together are injective, so step counts are logarithms in $\langle l \rangle \leq L^\times$ with $L = K$ or a quadratic extension of K ; for $c = \pm 1$ the Jordan closed form $\sigma^n(x, y) = l^n(x + \frac{n}{l}w, y + nw)$, $w = y - lx$, makes the step count a linear equation. Any non-scalar linear map C with $\det C = 1$ ($2 \neq 0$) is conjugate to the oscillator with $2c = \text{tr } C$, and an affine map $v \mapsto Cv + b$ with $\det C = 1$ and an isolated fixed point is linear in coordinates centred there; an affine map with $\text{tr } C = 2$ and no fixed point has one of the normal forms $(x, y) \mapsto (x + y, y + 1)$ and $(x, y) \mapsto (x, y + 1)$.

E2. The system called E2 in [18] is the Kahan discretisation of the geodesic flow of the Hessian metric of $-\log Q$ for a quadratic form Q with bilinear form B ; for $Q = x^2 - y^2 - z^2$ the geodesics on $Q = 1$ are those of the hyperbolic plane. The step is $(p, x) \mapsto (x, (2B(x, p)x - Q(x)p)/Q(p))$ on states with $Q(p)Q(x) \neq 0$, which never become singular. The quantities $r = Q(x)/Q(p)$, $b = B(p, x)/Q(p)$ and $\omega(p, x)/Q(p)$ for every alternating bilinear form ω are conserved; the orbit obeys $x_{k+1} = 2bx_k - rx_{k-1}$, so σ^k is the k th power of the companion matrix C , and for independent p, x the automorphism group of the state in the action groupoid is $\text{ord}(C)\mathbb{Z}$. The phase is given by the eigen-coordinates for the roots of $\lambda^2 - 2b\lambda + r$ or by the Jordan form.

Conjugacies. An isomorphism of partial flows (a bijection e with $f(x) = y \iff f'(ex) = ey$) preserves regularity, step counts, the absence of paths and partial orbits. The Lyness-type map $(x, y) \mapsto (y, (a + by)/x)$ and its reverse are the Lyness map with parameter a/b^2 after scaling; a system whose formulas become those of the Lyness map under a bijective change of coordinates is isomorphic to the Lyness flow; and since the Kahan step commutes with affine changes of coordinates, a quadratic vector field that is the Euler top in affine coordinates has a Kahan discretisation isomorphic to the top's. Examples A.8–A.10 rest on these theorems: a rational map or vector field given in unfamiliar coordinates is matched to the Lyness map or the Euler top, and only the polynomial identities behind the match need to be verified.

7 Regularity by the phase

The statements of the preceding sections concern regular states, and the hypothesis cannot be dropped: an orbit may reach a division by zero only after about 8.8×10^{17} steps (Example A.2).

On a level that carries a phase, the states at which the map is undefined are explicit and few, and regularity reduces to a membership question in the group.

Theorem 7.1. *Let (f, g) be a partial flow with a region R invariant along defined steps and $\psi : R \rightarrow A$ with $\psi(y) = \psi(x) + P$ whenever $f(x) = y$. Let $s \in R$.*

- (a) *If every $z \in R$ at which f or g is undefined has $\psi(z) - \psi(s) \notin \langle P \rangle$, then s is regular.*
- (b) *If ψ is injective on R and some such z has $\psi(z) - \psi(s) \in \langle P \rangle$, then s is not regular.*
- (c) *(Chains.) Under the hypotheses of (b), $f^n(s) = t$ for $n \geq 0$ if and only if $t \in R$, $\psi(t) = \psi(s) + nP$, and no forward-stuck $y \in R$ has $\psi(y) = \psi(s) + mP$ with $0 \leq m < n$; the same holds for g with $-P$ and the backward-stuck states.*

Proof. (a) A stuck $z = f^m(s)$ would have $\psi(z) = \psi(s) + mP$. (b) If $\psi(z) = \psi(s) + nP$ with f undefined at z and, say, $n \geq 0$: were s regular, $f^n(s)$ would be defined, lie in R and have the same ψ -value as z , hence equal z by injectivity. (c) If $f^n(s) = t$ then every $f^m(s)$ with $m < n$ is defined, so no forward-stuck state has one of those phases; conversely, if no forward-stuck state y has $\psi(y) = \psi(s) + mP$ for $m < n$, the iterates up to $f^n(s)$ are all defined by (a)'s argument, and $f^n(s) = t$ by injectivity. $\square$

The Lyness map. On the level k , T is undefined where $a + y = 0$; substituting $y = -a$ into the level equation gives $(1 - a)x = -(ka + 1 - a)$. So for $a \neq 1$ the level has at most one forward-stuck state $F = (-\frac{ka+1-a}{1-a}, -a)$ and one backward-stuck state $G = (-a, -\frac{ka+1-a}{1-a})$: a state is regular iff neither $\varphi(F) - \varphi(s)$ nor $\varphi(G) - \varphi(s)$ lies in $\langle Q \rangle$, two further logarithms or witnesses, and otherwise its chain and the step count to t are read off the logarithms of $\varphi(F) - \varphi(s)$, $\varphi(G) - \varphi(s)$ and $\varphi(t) - \varphi(s)$. The same holds on the nodal and reducible levels with their groups.

The Euler top. For the universal top the step is undefined where $D(u)D(-u) = 0$ or where the multiplier of y or its mirror vanishes. On the level with multiplier m ($y(u) = m\alpha$), with $r_i = 1 - m\alpha_i$,

$$P_D(m) = (1 - \sum r_i)^2 - 4r_1r_2r_3,$$

$$P_P(m) = ((1 + r_3 - r_1 - r_2)^2 + 4r_3 - 4r_1r_2)^2 - 16(1 + r_3 - r_1 - r_2)^2r_3$$

have degrees ≤ 3 and ≤ 4 , and under the substitution $r_i = u_i^2$ the first becomes $D(u)D(-u)$ and the second the product of the multiplier of T and that of T^{-1} . The stuck states are therefore among the u with $u_i = \pm\sqrt{1 - m\alpha_i}$ for a root m of P_DP_P : at most $7 \times 8 = 56$ candidates, found by root extraction. If no stuck candidate lies in the coset of $\psi(s)$, s is regular, for every top via the rescaling; a candidate in the coset that is stuck but takes two defined steps in the opposite direction shows s not regular.

8 Reduction to the rationals

Over $\mathbb{Q}$ orbits are in general infinite and logarithms are unavailable; we use reduction modulo primes instead.

Definition 8.1 (reduction). A reduction of a partial flow Φ to a partial flow Ψ is a partial map ρ such that whenever $\rho(x) = x'$ and $f_\Psi(x') = y'$ there is y with $f_\Phi(x) = y$ and $\rho(y) = y'$, and likewise for g .

Reduction modulo p of a rational map with p -integral data is a reduction in this sense: a nonzero reduced denominator is a p -adic unit upstairs.

Theorem 8.2 (reduction). *Let $\rho(s) = s'$, $\rho(t) = t'$. (a) If s' is regular, so is s . (b) If s' is regular, $\rho(\sigma^n s) = \sigma'^n s'$ for all n ; in particular $\sigma^n s = t$ implies $\sigma'^n s' = t'$. (c) If s' is regular and $\sigma'^n s' \neq t'$ for all n , then $\sigma^n s \neq t$ for all n .*

Composed along $\mathbb{Q} \rightarrow \mathbb{Q}_p \supseteq \mathbb{Z}_p \rightarrow \mathbb{Z}/p$ for the four families, this gives: for p -integral a, x, y , if $(\bar{x}, \bar{y})$ is a regular Lyness state over $\mathbb{Z}/p$ then (x, y) is regular over $\mathbb{Q}$; step counts over $\mathbb{Q}$ reduce modulo p ; and if $\bar{s}$ and $\bar{t}$ are never joined modulo p , then s and t are never joined over $\mathbb{Q}$. The same holds for the Euler top, the oscillator and E2 with a diagonal form Q .

The decision procedure over $\mathbb{Q}$. Given a bound B on $|n|$: choose primes above a starting point, skipping those at which the data are not p -integral or $\bar{s}$ is not regular; at each prime compute $\text{Id}(\bar{s}, \bar{t})$, regularity included. A “no path” at any prime is a *no path over $\mathbb{Q}$* , unconditional and independent of B , by (c). Otherwise combine the residue classes by the Chinese remainder theorem until the modulus exceeds $2B$; at most one candidate n with $|n| \leq B$ remains, which is confirmed by exact rational iteration or excluded. Regularity of $\bar{s}$ at the prime is essential: without it a path over $\mathbb{Q}$ could pass through a state that reduces to a division by zero. Examples A.4 and A.6 are of this kind: one prime at which the phases differ shows that the Lyness map with $a = 3$ never carries $(3, 7)$ to $(7, 3)$ over $\mathbb{Q}$, although both are positive and on one level, and that two states of the Euler top joined over $\mathbb{F}_q$ are never joined over $\mathbb{Q}$.

9 The type-theoretic content

Consider the following theory in Martin-Löf type theory, in the syntax of HoTTLean/SynthLean [17],

$$X : \mathcal{U}_0, \quad s, t : X, \quad \text{step} : X \rightarrow X, \quad \text{path} : \prod_{x:X} \text{Id}_X(x, \text{step } x).$$

It proves $\text{Id}(\text{step}^m s, \text{step}^n s)$ for all m, n (by path, J and reflexivity). Given any flow (S, σ) and states s_0, t_0 , the theory is interpreted in HoTTLean’s groupoid model by $X \mapsto S//\mathbb{Z}$, $s, t \mapsto s_0, t_0$, $\text{step} \mapsto \sigma$ (a functor, since σ commutes with the $\mathbb{Z}$ -action) and $\text{path} \mapsto (x \mapsto 1 : x \rightarrow \sigma x)$ (natural, since $\mathbb{Z}$ is commutative).

Theorem 9.1. *In the groupoid model the identity type $\text{Id}_X(s, t)$ is interpreted by $\text{Hom}_{S//\mathbb{Z}}(s_0, t_0) = \{n : \sigma^n s_0 = t_0\}$, the term $\text{step}^n s$ by $\sigma^n s_0$, and the loop space $\text{Id}(s, s)$ by the period subgroup. By the soundness of the interpretation, if t_0 is not on the orbit of s_0 —in particular if a conserved quantity or the phase differs—then no term of type $\text{Id}(\text{step}^m s, \text{step}^n t)$ is derivable.*

In this sense the results of Sections 3–8 compute identity types: the equivalences between hom-sets of the action groupoid and solution sets of the phase equations are proved in that form, rather than only as statements about iterates. A conjugacy e of flows is an isomorphism of action groupoids, and transport along it carries $\text{Id}(s, t)$ to $\text{Id}(es, et)$, preserving step counts, integrals and periods. This is the type-theoretic form of the conjugacies of Section 6 and of the system’s transport of checked results between conjugate systems.

10 The formalisation

10.1 Scope and statistics

The development is written in Lean 4 [7] on top of Mathlib [26] and HoTTLean, and comprises 1,146 theorems covering the abstract phase theorems, the four families level by level,

regularity, reduction, conjugacies and changes of coordinates, the semantics of systems given by formulas, the type-theoretic interpretation, and the executable checker with its soundness proof. There is no `sorry`, `admit`, `axiom` or `native_decide`; kernel computation is by `decide`. An automated audit of the axioms of every theorem finds only `propext`, `Classical.choice` and `Quot.sound`.

10.2 Proof technique

The elliptic identities of the Lyness map are polynomial identities conditional on the level equation (those of the top are unconditional); they are proved by `linear_combination` with explicit multipliers against Mathlib’s affine addition formulas, with the degenerate branches of the group law handled by case analysis, and were cross-checked symbolically and numerically by computer algebra before and after the formal proof. The group theory is Mathlib’s; the reduction lemma uses Mathlib’s p -adic integers; the degenerate levels use `AdjoinRoot` for quadratic extensions and quotient groups for $(K^\times \times \mathbb{Z})/\langle \cdot \rangle$.

10.3 Non-vacuity

A theorem with many hypotheses may be vacuous without anyone noticing. Each principal theorem is therefore instantiated at concrete states with every hypothesis discharged inside Lean: over $\mathbb{F}_{13}$ the Lyness map with $a = 2$ on the level $k = 11$ (a regular state, a non-regular one with its chain $(11, 8) \rightarrow (8, 8) \rightarrow (8, 11)$), the two reducible levels; over $\mathbb{F}_{17}$ the Euler top $(2, 2, 16, 10)$ with a regular and a non-regular state; over $\mathbb{Q}$ the states $(2, 5)$ (Lyness, $a = 3$) and $(1/3, 1/5, 1/7)$ (Euler top $(1, 2, -3, 1/2)$), regular by reduction from a cycle modulo 13; the Jordan and non-split oscillators; the conjugacy entries, including the cat map (of period 14 over $\mathbb{F}_{13}$) and an affine cat map. Where possible the same fact is also established directly, so that theorem and computation agree.

10.4 A certificate checker proved sound

The system described in [18] attaches to every answer a certificate (the level, the translation point, orders with factorisations, logarithms or non-membership witnesses, and regularity data) that an independent program checks. For the Lyness map over $\mathbb{F}_q$ that checker exists in a second form, written in core Lean without Mathlib at run time, together with the theorem that whatever it accepts is true: if the checker accepts a certificate, then q is prime and, over $\mathbb{Z}/q$, the claim holds of the Lyness flow as defined in the development—for *steps* (r, M) , that $\sigma^n s = t \iff n \equiv r \pmod{M}$ for the regular states; for *no path*, that $\sigma^n s \neq t$ for all n ; for *not regular*, that s is not regular with the stated chain length and that t is reached exactly at the stated n . The executable part verifies Pratt certificates of primality [22] with a proved Lucas test, uses the affine addition formulas (proved to agree with Mathlib’s group operations), checks orders by $NP = 0$ and $(N/\ell)P \neq 0$ for every prime $\ell \mid N$, and walks bounded distances for witnesses; it covers the elliptic and nodal levels with all regularity statuses and the partial orbits of non-regular states. Its corollaries connect it to Section 9: an accepted *steps* certificate gives an equivalence $\text{Id}(s, t) \simeq \{n : n \equiv r \pmod{M}\}$ in the action groupoid, and an accepted *no path* certificate gives the non-derivability of any identity.

11 Related work

The translation structure of QRT maps is due to Quispel, Roberts and Thompson [23, 24] and was treated exhaustively, singular fibres included, by Duistermaat [8]; Bastien and Rogalski

[3] described the real dynamics of the Lyness map on its level curves, and Hone [10, 11] used Lyness iteration as scalar multiplication for factorisation. The Hirota–Kimura discretisation [9] and its integrals were studied by Petrera and Suris [19] within the general theory of Kahan’s method [4, 20]. The present work builds on these: it supplies the explicit Weierstrass models and translation points for all levels (including W_α and the reduction of every top to the universal one), the complete treatment of the degenerate levels, the regularity criterion and the reduction theorem, and the formal proofs of all of it. The orbit problem for linear maps is Kannan–Lipton [14] and Chonev–Ouaknine–Worrell [6]; Lauter and Stange [15] connected index recovery in elliptic divisibility sequences to the elliptic discrete logarithm. Roberts and Vivaldi [25] and Jogia, Roberts and Vivaldi [12] study integrable maps over $\mathbb{F}_p$ through the statistics of their periods and the group orders of the fibres; the present paper computes the individual orbits. Mathlib’s Weierstrass curves [1] are the foundation of the formalisation; to our knowledge this is the first formalisation of a QRT or Kahan map and of elliptic discrete logarithms as a tool for dynamics in any proof assistant. The groupoid model and the certified interpretation are HoTTLean/SynthLean [17]; Awodey and Hua [2] inspired the project’s type-theoretic starting point. Verified checkers for certificates of untrusted solvers are an established pattern [5, 16]; Section 10.4 brings it to orbit certificates.

12 Scope and further work

The theory covers four families and their affine conjugates; a general QRT map preserves a pencil of elliptic curves, so Section 4 is a template for extending it, and higher-dimensional Kahan discretisations with enough integrals are the natural next targets. Point counting would lift the Euler top’s practical limit at $q \approx 2^{45}$ (reached when $h^2 a_2 a_3$ is a non-square). Extending the Lean-verified checker from the Lyness map to the other families and to $\mathbb{Q}$ is the next step on the formal side.

Use of AI

This work was carried out with an AI assistant (Claude, Anthropic) in a central role. The author set the goals, chose what to build and what to prove, made the design decisions and reviewed the results; under the author’s direction the AI assistant wrote most of the Lean development, the companion system and the text of this paper, verified the bibliography and took the measurements of Appendix A. The author is responsible for the content. The correctness of the mathematics rests on the Lean kernel and Mathlib, with the axioms audited and the principal theorems instantiated on concrete data.

Acknowledgements

The development builds on Lean 4, Mathlib and HoTTLean; the author thanks their contributors.

A Worked examples

The following are the “advanced examples” of the system’s site, recomputed on 22 October 2026 on a 2-core Intel Xeon at 2.1 GHz. Times are wall-clock for one command answering the question, including start-up, computation and the independent check (median of three runs).

For comparison, the same machine iterates the Lyness map over $\mathbb{F}_{2^{61}-1}$ at 2.6×10^6 steps/s and the Euler top over $\mathbb{F}_{2^{40}+15}$ at 2.4×10^6 steps/s. Here $q_{61} = 2^{61} - 1$ and $q_{40} = 1,099,511,627,791$.

Example A.1 (Lyness, $\mathbb{F}_{q_{61}}$: a state 7.9×10^{15} steps away). $a = 3$, $s = (2, 5)$, $t = (813066766938016773, 992646061924517494)$. Level $k = 18$; Q has order $576,460,752,629,115,698 = 2 \cdot 6673 \cdot 3612179 \cdot 11957747$ and $\log_Q(\varphi(t) - \varphi(s)) = 7,863,588,611,074,867$. Answer: $t = \sigma^n s \iff n \equiv 7,863,588,611,074,867 \pmod{576,460,752,629,115,698}$, both states regular by the phase test. 0.39 s. Iterating 7.86×10^{15} steps would take about 96 years; establishing the modulus by iteration about 73 times longer.

Example A.2 (Lyness, $\mathbb{F}_{q_{61}}$: a chain of length 8.8×10^{17}). $a = 3$,

$$s = (652450593252319644, 397870522539971473), \\ t = (557047722706213665, 1530465154515367894).$$

On the elliptic level $k = 1031421348935828000$, Q has order $2,305,843,011,612,193,701$, and the forward-stuck state has logarithm $881,059,717,639,816,779$ relative to s : s is not regular, its forward orbit meeting a division by zero after that many steps, and t is reached exactly at $n = 403,567,694,157,578,575$. 18.4 s, the time going into the arithmetic of the prime-order component of size about 2^{45} .

Example A.3 (Lyness, $\mathbb{F}_{q_{61}}$: same level, never reached). $a = 3$,

$$s = (1473736884130421033, 1913329524460333331), \\ t = (1744307874685056163, 461811991117244972).$$

Both states lie on the level $k = 471089872214466856$; Q has order $192,153,584,192,171,886 = 2 \cdot 3^2 \cdot 47 \cdot 17203 \cdot 70957 \cdot 186071$; $\varphi(t) - \varphi(s) \notin \langle Q \rangle$, witnessed in the 2-primary component. Answer: no path. 0.48 s. Iterating once around the orbit of s would take about 2,300 years.

Example A.4 (Lyness over $\mathbb{Q}$: $(3, 7)$ and $(7, 3)$). $a = 3$, bound 30. Both states are positive and on one level curve; the similar pair $(2, 5), (5, 2)$ is joined in 3 backward steps. At $p = 10009$, $\bar{s}$ is regular and the phases differ, so no integer n has $T^n(3, 7) = (7, 3)$ over $\mathbb{Q}$. 0.19 s.

Example A.5 (Euler top, $\mathbb{F}_{q_{40}}$: half the period). $(a_1, a_2, a_3, h) = (1, 2, -3, 1/2)$, $s = (3, 1, 4)$, $t = (3, -1, -4)$. Case A; Q has order $274,877,781,052 = 2^2 \cdot 7 \cdot 61 \cdot 7901 \cdot 20369$, logarithm $137,438,890,526$: the state with two signs changed is reached exactly at half the period. 0.35 s.

Example A.6 (Euler top over $\mathbb{Q}$: the same pair). Same data, bound 30. At $p = 10039$ the phases differ: the two states, joined over $\mathbb{F}_{q_{40}}$ and sharing both independent integrals, are never joined over $\mathbb{Q}$. 0.26 s.

Example A.7 (Euler top, $\mathbb{F}_{q_{40}}$: same integrals, never reached). $s = (3, 1, 4)$, $t = (-3, -1, 4)$ share both independent integrals; non-membership is witnessed in the elliptic component. Answer: no path. 0.42 s.

Example A.8 (A rational map of the plane, $\mathbb{F}_{q_{61}}$). $x' = -\frac{3x^2-5xy+x+2y^2-3y-2}{3x-2y+5}$, $y' = -\frac{3x^2-5xy-19x+2y^2+10y-33}{3x-2y+5}$, $s = (21, 33)$, $t = (492515881573357819, 1485161943497875320)$. The affine change of coordinates $u = (3x - 2y + 5, -x + y - 7)$ turns the formulas into the Lyness map with $a = 3$; the states become those of Example A.1 and the answer is the same residue class. 0.44 s.

Example A.9 (The same map over $\mathbb{Q}$). $s = (26, 40)$, $t = (22, 32)$, bound 30: Example A.4 in new coordinates. No path. 0.26 s.

Example A.10 (A quadratic field in three variables, Kahan step $h = 1/2$, $\mathbb{F}_{q_{40}}$). Three full quadratics with fractional coefficients (on the examples page), $s = (6, 4, 14)$, $t = (4, -6, -2)$. The centre (where all partial derivatives vanish) and the three axes (the zeros of the homogeneous part in $\mathbb{P}^2$) give the affine map to the Euler top $(-3, 2, 1)$, $h = 1/2$, which is the top of Example A.5 with the coordinates reversed, and the same answer. 0.41 s.

References

- [1] David Kurniadi Angdinata and Junyan Xu. An elementary formal proof of the group law on Weierstrass elliptic curves in any characteristic. In *14th International Conference on Interactive Theorem Proving (ITP 2023)*, volume 268 of *LIPICs*, pages 6:1–6:19. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2023. doi: 10.4230/LIPICs.ITP.2023.6.
- [2] Steve Awodey and Joseph Hua. Path types in algebraic type theory. arXiv:2601.06567, 2026.
- [3] G. Bastien and M. Rogalski. Global behavior of the solutions of Lyness’ difference equation $u_{n+2}u_n = u_{n+1} + a$. *Journal of Difference Equations and Applications*, 10(11): 977–1003, 2004. doi: 10.1080/10236190410001728104.
- [4] Elena Celledoni, Robert I. McLachlan, Brynjulf Owren, and G. R. W. Quispel. Geometric properties of Kahan’s method. *Journal of Physics A: Mathematical and Theoretical*, 46(2): 025201, 2013. doi: 10.1088/1751-8113/46/2/025201.
- [5] Krishnendu Chatterjee, Tim Quatmann, Maximilian Schäffeler, Maximilian Weininger, Tobias Winkler, and Daniel Zilken. Fixed point certificates for reachability and expected rewards in MDPs. arXiv:2501.11467, 2025.
- [6] Ventsislav Chonev, Joël Ouaknine, and James Worrell. On the complexity of the orbit problem. *Journal of the ACM*, 63(3):23, 2016. doi: 10.1145/2857050.
- [7] Leonardo de Moura and Sebastian Ullrich. The Lean 4 theorem prover and programming language. In *Automated Deduction – CADE 28*, volume 12699 of *Lecture Notes in Computer Science*, pages 625–635. Springer, 2021. doi: 10.1007/978-3-030-79876-5_37.
- [8] J. J. Duistermaat. *Discrete Integrable Systems: QRT Maps and Elliptic Surfaces*. Springer Monographs in Mathematics. Springer, New York, 2010. ISBN 978-1-4419-7116-6.
- [9] Ryogo Hirota and Kinji Kimura. Discretization of the Euler top. *Journal of the Physical Society of Japan*, 69(3):627–630, 2000. doi: 10.1143/JPSJ.69.627.
- [10] Andrew N. W. Hone. Efficient ECM factorization in parallel with the Lyness map. arXiv:2002.03811, 2020.
- [11] Andrew N. W. Hone. ECM factorization with QRT maps. In *Advances in Software Engineering, Education, and e-Learning*, Transactions on Computational Science and Computational Intelligence. Springer, 2021. doi: 10.1007/978-3-030-70873-3_28. arXiv:2001.09076 (2020).
- [12] Danesh Jogia, John A. G. Roberts, and Franco Vivaldi. An algebraic geometric approach to integrable maps of the plane. *Journal of Physics A: Mathematical and General*, 39(5): 1133–1149, 2006.

- [13] William Kahan. Unconventional numerical methods for trajectory calculations. Unpublished lecture notes, University of California, Berkeley, 1993.
- [14] R. Kannan and R. J. Lipton. Polynomial-time algorithm for the orbit problem. *Journal of the ACM*, 33(4):808–821, 1986. doi: 10.1145/6490.6496.
- [15] Kristin E. Lauter and Katherine E. Stange. The elliptic curve discrete logarithm problem and equivalent hard problems for elliptic divisibility sequences. In *Selected Areas in Cryptography (SAC 2008)*, volume 5381 of *Lecture Notes in Computer Science*, pages 309–327. Springer, 2009. doi: 10.1007/978-3-642-04159-4_20. arXiv:0803.0728.
- [16] Ross M. McConnell, Kurt Mehlhorn, Stefan Näher, and Pascal Schweitzer. Certifying algorithms. *Computer Science Review*, 5(2):119–161, 2011. doi: 10.1016/j.cosrev.2010.09.009.
- [17] Wojciech Nawrocki, Joseph Hua, Mario Carneiro, Yiming Xu, Spencer Woolfson, Shuge Rong, Sina Hazratpour, and Steve Awodey. A certifying proof assistant for synthetic mathematics in Lean. In *Proceedings of the 15th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2026)*. ACM, 2026.
- [18] Yuta Ogura. Structure Computer: certified structure computation for discrete dynamical systems. Companion paper, same site, 2026.
- [19] Matteo Petrera and Yuri B. Suris. On the Hamiltonian structure of Hirota–Kimura discretization of the Euler top. *Mathematische Nachrichten*, 283(11):1654–1663, 2010. doi: 10.1002/mana.200711162. arXiv:0707.4382.
- [20] Matteo Petrera, Andreas Pfadler, and Yuri B. Suris. On integrability of Hirota–Kimura type discretizations. *Regular and Chaotic Dynamics*, 16(3–4):245–289, 2011. doi: 10.1134/S1560354711030051.
- [21] Stephen C. Pohlig and Martin E. Hellman. An improved algorithm for computing logarithms over $\text{GF}(p)$ and its cryptographic significance. *IEEE Transactions on Information Theory*, 24(1):106–110, 1978. doi: 10.1109/TIT.1978.1055817.
- [22] Vaughan R. Pratt. Every prime has a succinct certificate. *SIAM Journal on Computing*, 4(3):214–220, 1975. doi: 10.1137/0204018.
- [23] G. R. W. Quispel, J. A. G. Roberts, and C. J. Thompson. Integrable mappings and soliton equations. *Physics Letters A*, 126(7):419–421, 1988. doi: 10.1016/0375-9601(88)90803-1.
- [24] G. R. W. Quispel, J. A. G. Roberts, and C. J. Thompson. Integrable mappings and soliton equations II. *Physica D*, 34(1–2):183–192, 1989. doi: 10.1016/0167-2789(89)90233-9.
- [25] John A. G. Roberts and Franco Vivaldi. Arithmetical method to detect integrability in maps. *Physical Review Letters*, 90(3):034102, 2003. doi: 10.1103/PhysRevLett.90.034102.
- [26] The mathlib Community. The Lean mathematical library. In *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020)*, pages 367–381. ACM, 2020. doi: 10.1145/3372885.3373824.