THE LENGTH SPECTRUM OF q-DISCRETE PAINLEVÉ I OVER A FINITE FIELD: AN EXACT FORM OF THE BIN CONJECTURE AT PRIME q, AND VERIFICATION PAST THE PUBLISHED RANGE

KOREA SUPERINTELLIGENCE LABS

Abstract. Joshi and Roffelsen have shown that the q-discrete first Painlevé equation, resolved on Sakai's initial value space, defines a bijection of a set of $(q+1)^2$ points over a finite field $\mathbb{F}_q$, and they conjecture on the strength of a Magma computation over every prime power $2 \le q \le 499$ that every reduced orbit length obeys the Hasse bound $q + 2\sqrt{q} + 1$ and in fact lies in one of M_q explicit disjoint intervals, the *bins*. We report four things about the set of reduced orbit lengths that is actually realised. First, for every prime q with $3 \le q \le 131$ the conjectured containment is an *equality*: every integer in every bin other than 2 and 3 occurs as a reduced orbit length, and nothing else does. This fails at the proper prime powers $q = 4, 9, 25, 128$, so the phenomenon is one of prime q. Second, the largest reduced orbit length is exactly $q + 1 + \max\{d \in \mathbb{N} : d^2 < 4q\}$, the largest integer strictly below the Hasse bound, at every prime power $q \le 131$ except $q = 128$, where it falls one short. Third and fourth, both conjectures hold for all 3 534 638 orbits over $\mathbb{F}_{503}$, the first prime power past the published range, and for all 5 756 256 orbits over $\mathbb{F}_{1009}$ whose parameter s is one of the twelve smallest elements of $\mathbb{F}_{1009}^{\times}$, where $M_q = 8$ against $M_{499} = 6$. All statements are formally verified in Lean 4; every search is exhaustive over the range stated and is described.

1. Introduction

The equation, and the space it acts on. Fix a prime power $q = p^n$ and elements $s, t \in \mathbb{F}_q^{\times}$. The q-discrete first Painlevé equation in the form studied by Joshi and Roffelsen [1] is the birational map

$$\bar{x} = \frac{t}{x - s^{-1}y}, \qquad \bar{y} = \frac{sx}{y}, \qquad \bar{t} = st, \tag{1}$$

acting on a pair of coordinates on $\mathbb{P}^1 \times \mathbb{P}^1$ together with a time coordinate that advances geometrically. The map is ill defined at eight base points. Following Sakai's construction of initial value spaces for the discrete Painlevé equations [5], [1, Definition 2.1] blows those points up and deletes the coordinate lines, obtaining the *initial value space* $X_{t,s}$ on which (1) becomes a bijection $X_{t,s} \to X_{st,s}$.

Over $\mathbb{F}_q$ the rational points of $X_{t,s}$ admit the following bookkeeping, which is [1, Definition 2.2] with the fixed parameter s suppressed from the tuple. A *state* is a tuple (j, x, y, t) with $t \in \mathbb{F}_q^{\times}$ and either

- $j = 0$ and $(x, y) \in \mathbb{F}_q^{\times} \times \mathbb{F}_q^{\times}$ — an ordinary point; or
- $1 \le j \le 4$, $x = 0$ and $y \in \mathbb{F}_q$ — a point of the exceptional line L_j.

Hence

$$\#X_{t,s}(\mathbb{F}_q) = (q-1)^2 + 4q = (q+1)^2, \tag{2}$$

and the time evolution, which is Algorithm 1 of [1], is a bijection of this set of $(q+1)^2$ states onto the corresponding set for the time st. Since $t \mapsto st$ has period $r := \mathrm{ord}(s)$, the r-fold composite is an *automorphism* of the single space $X_{t,s}$. Writing $\#(\gamma)$ for the number of states of an orbit γ of the evolution, [1, Definition 1.1(iii)] observes that "the multiplicative order r of s must be a divisor of both $q-1$ and $\#(\gamma)$", so the *reduced orbit length* $\#(\gamma)/r$ is an integer; it is exactly an orbit length of the r-fold composite acting on $X_{t,s}$. Proposition 2.2 below proves the divisibility over an arbitrary field.

The two conjectures, and what is open. The two central assertions of [1] are conjectures. With γ an orbit of (1) over $\mathbb{F}_q$ and $r = \mathrm{ord}(s)$:

Conjecture A ([1, Conjecture 1.2.A])**.** $\#(\gamma)/r \le q + 2\sqrt{q} + 1$.

Conjecture B ([1, Conjecture 1.2.B])**.** $\#(\gamma)/r$ lies in one of the M_q disjoint intervals

$$B_m = \left[\tfrac{q+1-2\sqrt{q}}{m},\ \tfrac{q+1+2\sqrt{q}}{m}\right] \quad (1 \le m \le M_q - 1), \qquad B_{M_q} = \left[1,\ \tfrac{q+1+2\sqrt{q}}{M_q}\right],$$

where $M_q = \lceil (\sqrt{q} + 1/\sqrt{q} - 2)/4 \rceil$.

The bound of Conjecture A is the Hasse bound for the number of $\mathbb{F}_q$-points of a genus-one curve, and that is not a coincidence: [1, Theorem 3.1] constructs, for every s of finite multiplicative order r, a rational integral of motion I_r of (1) built from the trace of a product of r Lax matrices in the form of Murata [6], and [1, Conjecture 3.6] asserts that the fibres of I_r have geometric genus one away from an explicit quartic locus. Version 2 of [1] adds a remark, absent from v1, that Conjecture 3.6 implies the Hasse upper bound of Conjecture A. Both remain open. The evidence offered for Conjecture 1.2 is computational: a Magma [9] verification over more than 200 million orbits, "with the prime power q ranging from 2 to 499" [1, §1.1], whose orbit data is deposited separately [4].

Two 2026 papers by the same group cite [1], and to our knowledge they are the only papers that do; neither proves either conjecture and neither extends the verified range. The first [2] constructs integrals of motion for $\mathrm{P_{IV}}$ and for the difference $\mathrm{P_{II}}$ in finite characteristic and describes [1] in its introduction as having "checked for more than 200M orbits over finite fields that they satisfy an analogue of the Hasse bound". The second [3] writes that in [1] the orbits "are shown to lie on certain algebraic curves, conjectured to generally be elliptic curves". As of July 2026 the curve statement is still called a conjecture by its authors.

What is settled here. This paper proves neither conjecture. What it does is describe the realised length spectrum exactly on a certified range, and push the verification past the published one. Write

$$\mathcal{R}(q) = \left\{ \#(\gamma)/r \ :\ \gamma \text{ an orbit of (1) over } \mathbb{F}_q,\ s \in \mathbb{F}_q^{\times},\ r = \mathrm{ord}(s) \right\}, \qquad \mathcal{B}(q) = B_1 \cup \cdots \cup B_{M_q},$$

so that Conjecture B reads $\mathcal{R}(q) \subseteq \mathcal{B}(q)$. Set

$$H(q) \ :=\ q + 1 + \max\{d \in \mathbb{N} : d^2 < 4q\}, \tag{3}$$

the largest integer *strictly* below the Hasse bound $q+2\sqrt{q}+1$. For non-square q this is $\lfloor q+2\sqrt{q}+1 \rfloor$, since $4q$ is then not a square; for square q it is one less, the bound $(\sqrt{q}+1)^2$ being an integer there.

Theorem 1.1 (Theorem 5.1)**.** *For every prime q with $3 \le q \le 131$,*

$$\mathcal{R}(q) = \mathcal{B}(q) \setminus \{2, 3\}.$$

That is, every integer lying in one of the M_q bins, other than 2 and 3, is the reduced length of some orbit of (1) over $\mathbb{F}_q$, and no other integer is. The equality fails at the proper prime powers $q = 4$, 9, 25 and 128.

Theorem 1.2 (Theorems 4.1 and 4.2)**.** *For every prime power q with $2 \le q \le 131$ except $q = 128$, the largest reduced orbit length of (1) over $\mathbb{F}_q$ is exactly $H(q)$. At $q = 128$ it is 150, whereas $H(128) = 151$.*

Theorem 1.3 (Theorems 6.1 and 6.2)**.** *Conjectures A and B hold for all 3 534 638 orbits of (1) over $\mathbb{F}_{503}$ — every $s \in \mathbb{F}_{503}^{\times}$ and every coset of $\langle s \rangle$ — with largest reduced orbit length $548 = H(503)$ and smallest 1. They hold for all 5 756 256 orbits over $\mathbb{F}_{1009}$ with $s \in \{1, \ldots, 12\}$, with largest reduced orbit length $1073 = H(1009)$ and smallest 1; there $M_{1009} = 8$.*

Theorem 1.1 is the substantial one. Conjecture B is an upper envelope; Theorem 1.1 says that on its certified range the bins are not an envelope at all but the exact shape of the spectrum, and that this is a phenomenon of prime q. It implies Theorem 1.2 at every prime $q > 2$ (Corollary 5.3), and

it is a much more rigid target for a structural explanation: any account of Conjecture B by counting points on the fibres of the integral of motion must reproduce not just an inequality but a surjection onto each bin.

Theorem 1.3 moves the verification past $q = 499$. The cost of a complete cell is exactly $(q^2-1)^2$ evolution steps — $(q+1)^2(q-1)$ per value of s, uniformly in s — so it is quartic in q and the frontier moves slowly; $q = 503$ is 6.40×10^{10} steps. At $q = 1009$ a complete sweep is 1.04×10^{12} steps and was not run, but a complete sweep for one fixed s is self-contained: for that s the orbits found partition $X_{t_0,s}$ as t_0 runs over all $(q-1)/r$ cosets of $\langle s\rangle$ in $\mathbb{F}_q^\times$, so *every* orbit with that s is accounted for. Theorem 1.3 is complete in that sense for twelve values of s whose multiplicative orders realise six distinct divisors of 1008, including a primitive root.

Novelty, and what is not claimed. We claim no priority for Conjectures A and B, for the bin arithmetic, or for the numerical data inside $2 \le q \le 499$, all of which is [1]'s. Two points of provenance need stating explicitly.

First, the exclusion of the values 2 and 3 in Theorem 1.1 is *not* new. A remark to the effect that an orbit with reduced length 2 or 3 was never encountered sits **commented out** in the LaTeX source of both v1 and v2 of [1], and appears in neither compiled version; the authors evidently observed it and withheld it. We reproduce it here because Theorem 1.1 cannot be stated without it, and we attribute it to them. What is new in Theorem 1.1 is that *nothing else* is missing, and that the property separates prime q from proper prime powers.

Second, all four statements above are the outcome of a search of the literature that returned nothing, and we report them as such rather than as claims of novelty. What was searched: the full text of [1] in both versions, including every commented-out block of the LaTeX source, for the bin conjecture and for the words *maximum*, *sharp* and *attained*; the full text of the two follow-ups [2, 3]; the citation list of [1], which has exactly the two entries just named; the deposited orbit data [4], whose range [1, §2.3] again gives as $2 \le q \le 499$; the integer sequence databases for the sequence of maxima; and a local full-text arXiv corpus for the phrase *reduced orbit length*, which returned three documents, one of them [1] and the other two using the phrase in unrelated senses. The negatives should be read as "not found", not as "new".

Organisation. Section 2 fixes the evolution and proves the divisibility that makes the reduced length an integer. Section 3 puts Conjecture B into exact integer arithmetic and proves the bins disjoint. Sections 4, 5 and 6 prove Theorems 1.2, 1.1 and 1.3. Section 7 records the reproduction of [1]'s printed data and the negative controls, and Section 8 says what the formal verification covers and what it does not.

2. The evolution and the reduced orbit length

Throughout, F is a field, $s \in F^\times$, and a *state* over F is a tuple $g = (j, x, y, t)$ with $j \in \{0,1,2,3,4\}$ and $x, y, t \in F$, subject to $x = 0$ when $j \neq 0$. The following is Algorithm 1 (Time Evolution) of [1], written over F; the eight base points of (1) have been resolved into the four exceptional lines $L_1, \dots, L_4$, indexed by j.

Definition 2.1. The *evolution* φ_s sends $g = (j, x, y, t)$ to the state with time st and

$$\varphi_s(g) = \begin{cases} \big(0,\ t/(x - s^{-1}y),\ sx/y,\ st\big), & j = 0,\ sx \neq y, \\ \big(1,\ 0,\ t/x,\ st\big), & j = 0,\ sx = y, \\ \big(2,\ 0,\ st\,(1 - sy),\ st\big), & j = 1, \\ \big(3,\ 0,\ sy,\ st\big), & j = 2, \\ \big(4,\ 0,\ s(sy - t)/t,\ st\big), & j = 3, \\ \big(0,\ -s^2 t/y,\ 1,\ st\big), & j = 4,\ y \neq 0, \\ \big(1,\ 0,\ 0,\ st\big), & j = 4,\ y = 0. \end{cases}$$

The first branch is (1) itself; the remaining six are the resolution. Over $\mathbb{F}_q$, φ_s restricts to a bijection $X_{t,s} \to X_{st,s}$ between sets of $(q+1)^2$ states.

Proposition 2.2. *Let F be any field, $s \in F^\times$ and g a state over F with $t \neq 0$.*

(i) *Every branch of φ_s multiplies the time by s; consequently the time coordinate of $\varphi_s^m(g)$ is $s^m t$ for all $m \geq 0$.*
(ii) *If $\varphi_s^m(g) = g$ then $\mathrm{ord}(s) \mid m$.*
(iii) *If moreover $s \neq 1$ then $\varphi_s(g)$ and g have different times; in particular the system is genuinely non-autonomous and the reduction by r is not the identity.*

Proof. Part (i) is a case check on the seven branches of Definition 2.1, each of which writes the new time as st, followed by an induction on m. For (ii), $\varphi_s^m(g) = g$ gives $s^m t = t$, and cancelling $t \neq 0$ gives $s^m = 1$, so the order of s divides m. Part (iii) is the same cancellation. Nothing here is finite: no hypothesis on F, on s or on the orbit is used. □

Part (ii) is the remark of [1, Definition 1.1(iii)], and it is what makes the reduced orbit length an integer. Over $\mathbb{F}_q$ it has the following consequence, which is the shape of every computation below. Fix $s \in \mathbb{F}_q^\times$ and let $r = \mathrm{ord}(s)$. The composite φ_s^r is an automorphism of the single space $X_{t_0,s}$ for each $t_0 \in \mathbb{F}_q^\times$, and $X_{t_0,s} = X_{t_1,s}$ as sets of states exactly when t_0 and t_1 lie in the same coset of $\langle s \rangle$ in $\mathbb{F}_q^\times$. Hence:

Lemma 2.3. *Fix $s \in \mathbb{F}_q^\times$ and $r = \mathrm{ord}(s)$, and let t_0 run over one representative of each of the $(q-1)/r$ cosets of $\langle s \rangle$ in $\mathbb{F}_q^\times$. Decomposing each $X_{t_0,s}$ into orbits of φ_s^r produces every reduced orbit length of (1) over $\mathbb{F}_q$ with that s, each exactly once, and the lengths obtained from a single t_0 sum to $(q+1)^2$.*

Proof. An orbit γ of φ_s meets $X_{t_0,s}$ for exactly the t_0 in one coset, and meets it in a single φ_s^r-orbit of $\#(\gamma)/r$ states. Conversely every φ_s^r-orbit in $X_{t_0,s}$ arises this way. The sum is (2). □

The identity "lengths sum to $(q+1)^2$" is not decorative: it is the completeness check that every computation below carries, and it is what turns a search into a proof that nothing was missed. The cost of the decomposition for one s is $(q+1)^2(q-1)$ evolution steps, independent of $\mathrm{ord}(s)$, so a complete cell costs $(q^2-1)^2$ steps and equal ranges of s are equal-cost.

3. The bins in exact integer arithmetic

Conjectures A and B are statements about real numbers. Every computation in this paper is over $\mathbb{Z}$, so the first thing to fix is that the integer conditions tested are the real conditions stated. For $q, L, m, M \in \mathbb{N}$ put

$$\mathrm{hasse}(q, L) :\iff L \leq q+1 \ \text{ or } \ (L-(q+1))^2 \leq 4q, \tag{4}$$

$$\mathrm{bin}(q, m, L) :\iff (mL-(q+1))^2 \leq 4q \quad \text{(as an identity in } \mathbb{Z}), \tag{5}$$

and let $\mathrm{mq}(q)$ be the least $M \geq 1$ with $(2M+1)^2 \cdot 4q \geq (q+1)^2$.

Proposition 3.1. *Let $q, L, m, M \in \mathbb{N}$.*

(i) *$\mathrm{hasse}(q, L)$ holds if and only if $L \leq q + 2\sqrt{q} + 1$ in $\mathbb{R}$.*
(ii) *For $m < M$, the test used in the computations for membership of L in the m-th bin is exactly the integer inequality (5).*
(iii) *For $m \geq 1$, (5) holds if and only if $\frac{q+1-2\sqrt{q}}{m} \leq L \leq \frac{q+1+2\sqrt{q}}{m}$, that is, if and only if $L \in B_m$.*

Proof. All three are elementary. For (i), if $L > q+1$ then squaring is monotone on the nonnegative reals and $(L-(q+1))^2 \leq 4q \iff L-(q+1) \leq 2\sqrt{q}$; if $L \leq q+1$ both sides hold. For (ii), the computations evaluate $|mL-(q+1)|$ by a case split on the sign, natural-number subtraction being truncated; the two cases recombine to (5) over $\mathbb{Z}$. For (iii), multiply through by $m > 0$ and square as in (i). Parts (i) and (iii) are proved formally against Mathlib's real square root, so that

the machine-checked statements below assert Conjecture A and Conjecture B and not merely an integer shadow of them. □

Proposition 3.2. *Let $q \geq 0$ and $m \geq 1$ be integers and suppose some L satisfies both $(mL-(q+1))^2 \leq 4q$ and $((m+1)L-(q+1))^2 \leq 4q$. Then $(q+1)^2 \leq 4(2m+1)^2 q$, that is, $\mathrm{mq}(q) \leq m$. Consequently for $m < \mathrm{mq}(q)$ the bins B_m and B_{m+1} are disjoint.*

Proof. Put $a = mL-(q+1)$ and $b = (m+1)L-(q+1)$, so that $mb-(m+1)a = q+1$ identically. From $a^2 \leq 4q$, $b^2 \leq 4q$ and $-2ab \leq a^2+b^2$ one gets

$$(q+1)^2 = (mb-(m+1)a)^2 = m^2b^2 + (m+1)^2a^2 + m(m+1)\,(-2ab) \leq 4(2m+1)^2 q.$$

The last inequality is the definition of $\mathrm{mq}(q)$ being at most m. □

This is the word "disjoint" in Conjecture B turned into a proof, and it is what makes "the bin containing L" well defined below M_q. It also shows that Conjecture B is strictly stronger than Conjecture A as soon as $M_q \geq 2$: the bins then leave gaps inside $[1, q+2\sqrt{q}+1]$. Proposition 7.2(iii) exhibits such a gap.

Proposition 3.3. $\mathrm{mq}(33) = 1$, $\mathrm{mq}(34) = \mathrm{mq}(97) = 2$, $\mathrm{mq}(98) = \mathrm{mq}(193) = 3$, $\mathrm{mq}(194) = 4$ *and* $\mathrm{mq}(499) = 6$. *For $q = 499$ the integer endpoints of the six bins are*

$$[456, 544], \quad [228, 272], \quad [152, 181], \quad [114, 136], \quad [92, 108], \quad [1, 90],$$

which are the six intervals printed in [1, §2.4].

Proof. Direct evaluation of mq and of (5) at the seven values of q listed and, for $q = 499$, at every integer L in $[1, 2q+2]$. No orbit computation is involved. □

The seven values pin the whole step function, because mq is non-decreasing: $\mathrm{mq}(q) \leq m$ says $(q+1)^2 \leq 4(2m+1)^2 q$, i.e. $\left((\sqrt{q}+1/\sqrt{q})/2\right)^2 \leq (2m+1)^2$, and $\sqrt{q}+1/\sqrt{q}$ is non-decreasing for $q \geq 1$. Hence $M_q = 1$ for $q \leq 33$, $M_q = 2$ for $34 \leq q \leq 97$, $M_q = 3$ for $98 \leq q \leq 193$ and $M_q \geq 4$ for $q \geq 194$. This monotonicity is proved here rather than by computation, and it is the only place in the paper where a step of that kind is used.

It remains to say why the integer mq is the M_q of Conjecture B.

Proposition 3.4. *For every integer $q \geq 2$,*

$$\mathrm{mq}(q) = \left\lceil \tfrac{1}{4}\left(\sqrt{q}+1/\sqrt{q}-2\right) \right\rceil = M_q.$$

Proof. Let $M \geq 0$ be an integer. Both $2\sqrt{q}\,(2M+1)$ and $q+1$ are positive, so squaring is an equivalence on them, and

$$\begin{aligned} 4q(2M+1)^2 \geq (q+1)^2 &\iff 2\sqrt{q}\,(2M+1) \geq q+1 \iff 4M\sqrt{q} \geq q+1-2\sqrt{q} \\ &\iff M \geq \frac{q+1-2\sqrt{q}}{4\sqrt{q}} = \frac{\sqrt{q}+1/\sqrt{q}-2}{4}, \end{aligned}$$

the last step dividing by $4\sqrt{q} > 0$. So the least integer $M \geq 0$ satisfying the leftmost inequality is exactly the ceiling on the right. That ceiling is at least 1 for every $q \geq 2$, since $\sqrt{q}+1/\sqrt{q} > 2$ whenever $q \neq 1$; hence the least $M \geq 1$ satisfying the leftmost inequality — which is $\mathrm{mq}(q)$ — is the same integer. □

Two things should be said about Proposition 3.4. It is the one bridge between the integer arithmetic of this section and the source's real-number definition that is proved here by hand and is *not* among the formally verified statements of this development; unlike Proposition 3.1(i) and (iii) it has no Lean counterpart, and Section 8 lists it among the exceptions. Nothing downstream depends on it: every occurrence of M_q below is the integer mq, and the theorems assert what that integer says. Its one published cross-check is Proposition 3.3, which evaluates $\mathrm{mq}(499) = 6$ and the six bins that go with it, and those are the M_q and the bins [1, §2.4] prints.

4. The maximum reduced orbit length

[1, §1.1] remarks, just after Conjecture 1.2 and the remark on the autonomous case, that the bound "is sharp for many of the values of q and r included", and prints no table of maxima. The maxima are exact, and the exact value is not the floor of the Hasse bound.

Theorem 4.1. *Let q be a prime power with $2 \le q \le 131$ and $q \neq 128$. Then Conjectures A and B hold for every orbit of (1) over $\mathbb{F}_q$, and the largest reduced orbit length is exactly $H(q) = q + 1 + \max\{d : d^2 < 4q\}$.*

Proof sketch. This rests on exhaustive computation. For each of the 44 prime powers in the range the computation runs the decomposition of Lemma 2.3 for every $s \in \mathbb{F}_q^\times$ and every coset representative t_0, and asserts a single Boolean per q which fuses four things: that the tables presenting $\mathbb{F}_q$ audit correctly against the defining polynomial; that the reduced lengths obtained from each $X_{t_0,s}$ sum to $(q+1)^2$, so that no orbit was missed; that every reduced length satisfies (4) and lies in some bin; and that the largest reduced length equals $H(q)$. The search is 2.09×10^9 evolution steps and covers 3 222 405 orbits. Nothing is sampled: the quantifier over s, over t_0 and over the $(q+1)^2$ states of each $X_{t_0,s}$ is exhausted in every cell. □

Theorem 4.2. *Over $\mathbb{F}_{128} = \mathbb{F}_2[X]/(X^7 + X + 1)$ both conjectures hold for every orbit, the smallest reduced orbit length is 1, and the largest is 150. But $H(128) = 151$. Thus $q = 128$ is the unique prime power $q \le 131$ at which the maximum falls short of the largest integer strictly below the Hasse bound.*

Proof sketch. The complete sweep over $\mathbb{F}_{128}$, of the same shape as in Theorem 4.1, together with the arithmetic evaluation $H(128) = 151$ (equivalently, $22^2 = 484 < 512$ and $23^2 = 529 > 512$). The exception is intrinsic and not an artefact of the presentation of the field: an isomorphism of finite fields carries orbits to orbits of the same length, and the sweep ranges over all $s \in \mathbb{F}_{128}^\times$ and all cosets, so the multiset of reduced orbit lengths does not depend on which irreducible polynomial is used. The audit of the field tables against the defining polynomial rules out a mis-specified presentation separately. □

Two features of Theorem 4.1 are worth isolating. The first is that the *strict* form in (3) is forced by the data. At the eight perfect squares in the range, $q = 4, 9, 16, 25, 49, 64, 81, 121$, the Hasse bound $(\sqrt{q}+1)^2$ is itself an integer, and it is never attained: the maximum is exactly one less. A formula stated as $\lfloor q + 2\sqrt{q} + 1 \rfloor$ is therefore wrong at every square q in the range, while H is right at all of them. The second is that $q = 128$ is a genuine exception rather than a symptom of characteristic two: $q = 16, 32, 64$ are not exceptions. Whether 128 is isolated is open; the smallest computation that would decide it is $q = 256$.

Proposition 4.3. *For $q = 2, 3, 5, 7$ the largest reduced orbit length is $5, 7, 10, 13$ respectively, and these are $H(2), H(3), H(5), H(7)$. Both conjectures hold for every orbit over $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5, \mathbb{F}_7$.*

Proof sketch. A second, independent exhaustive computation over the four smallest prime fields, described in Section 8; it walks every one of the $(q+1)^2$ states of every $X_{t_0,s}$ as a start point rather than tracking which have been visited, and uses modular arithmetic rather than logarithm tables for the field. It agrees with the computation of Theorem 4.1 on all four maxima. □

The sharpness statement extends to the two cells beyond the published range: $H(503) = 548$ and $H(1009) = 1073$, which are the maxima found in Theorems 6.1 and 6.2 — the latter over the twelve values of s that theorem covers.

5. For prime q the bins are filled

Conjecture B is a containment. On the range certified here it is an equality, up to the two values the authors of [1] had already noticed to be absent.

Theorem 5.1. *Let q be a prime with $3 \le q \le 131$. Then*

$$\mathcal{R}(q) = \mathcal{B}(q) \setminus \{2, 3\} :$$

an integer $L \ge 1$ is the reduced length of some orbit of (1) over $\mathbb{F}_q$ if and only if L lies in one of the M_q bins and $L \notin \{2, 3\}$.

Proof sketch. Exhaustive computation, over the 31 primes in the range; 1.57×10^9 evolution steps. For each q the frequency array of reduced orbit lengths is assembled by summing, over every divisor r of $q-1$, the frequency list of [1, §2.3] for that r — namely the multiset of reduced lengths over every $s \in \mathbb{F}_q^\times$ of order r and every coset of $\langle s \rangle$. By Lemma 2.3 that sum counts every orbit of (1) over $\mathbb{F}_q$ exactly once, so its support is $\mathcal{R}(q)$. The test then compares, for every integer L with $1 \le L \le 2q+3$, the Boolean "L is realised" against the Boolean "L lies in a bin and $L \ne 2, 3$", and requires them equal. The field tables are audited first, as in Theorem 4.1. This settles the statement on $[1, 2q+3]$, and that suffices: on one side $\mathcal{B}(q) \subseteq [1, q + 2\sqrt{q} + 1] \subseteq [1, 2q+3]$, and on the other every element of $\mathcal{R}(q)$ lies in $[1, q + 2\sqrt{q} + 1]$ by Theorem 4.1, whose range includes all 31 of these primes. Both containments are therefore checked, and both are exhaustive; no part of the statement is sampled. □

Theorem 5.2. *The equality of Theorem 5.1 fails at $q = 4$, $q = 9$, $q = 25$ and $q = 128$. It also fails at $q = 2$: there $\mathbb{F}_2^\times = \{1\}$, the space $X_{1,1}$ decomposes into exactly two orbits, of reduced lengths 4 and 5, and $B_1 = [1, 5]$, so 1 is missing as well as 2 and 3.*

Proof sketch. Four complete sweeps of the shape used in Theorem 5.1, at $q = 4, 9, 25, 128$, each returning that the realised set differs from $\mathcal{B}(q) \setminus \{2, 3\}$; and one at $q = 2$ together with the evaluation $B_1 = [1, 5]$. □

Corollary 5.3. *For every prime q with $3 \le q \le 131$, the largest reduced orbit length over $\mathbb{F}_q$ is $H(q)$. In particular Theorem 5.1 implies the prime case of Theorem 4.1.*

Proof. No prime $q > 2$ is a square, so $4q$ is not a square and the largest integer in B_1 is $H(q)$ by Proposition 3.1(iii); it exceeds 3, so Theorem 5.1 puts it in $\mathcal{R}(q)$. It is also the largest element of $\mathcal{B}(q)$, hence of $\mathcal{R}(q)$. □

Remark 5.4 (The two absent values are the authors' observation). The exclusion of 2 and 3 in Theorem 5.1 is not offered as new. A remark reading, in substance, that an orbit with $\#(\gamma)/r$ equal to 2 or 3 was never encountered sits commented out in the LaTeX source of both versions of [1] and appears in neither compiled version, alongside a commented-out conjecture to the same effect. Our data agrees with it in every cell computed for this paper: in all of them the realised set contains 1 and then jumps to 4. We record this as the authors' observation, withheld by them, and claim only the complementary half of Theorem 5.1, that nothing beyond $\{2, 3\}$ is missing at prime q. A proof of the $\{2, 3\}$ half looks within reach and is not attempted here: reduced length 1 is a fixed point of φ_s^r, and the apparent floor at 4 has the length of the chain $L_1 \to L_2 \to L_3 \to L_4$ in Definition 2.1.

Remark 5.5 (What fails at a proper prime power, and a mechanism worth testing). Theorem 5.2 says only that the equality fails. The shape of the failure — read off the same frequency data, but computed by the unverified reference implementation of Remark 6.3 and part of no certified statement here — is that at $q = 4, 9, 25$ the single extra missing value is the Hasse bound $(\sqrt{q}+1)^2$ itself, that is, 9, 16 and 36. This is consistent with Theorem 4.1, which already asserts that the maximum at a square q is $(\sqrt{q}+1)^2 - 1$. At $q = 128$ the bins hold 117 integers and 26 of them are unrealised: 2 and 3, and then twenty-four further values, namely 39, 41, 45, 47, 49 and nineteen of the odd integers of $B_1 = [107, 151]$.

A mechanism suggests itself, and we state it as a question and not as a claim. By [1, Theorem 3.1, Conjecture 3.6] the orbits lie on fibres of an integral of motion that are conjecturally genus-one curves, so a realised reduced length should have the shape N/m with N the number of $\mathbb{F}_q$-points of such a curve. Which N occur is classical. Waterhouse classifies the isogeny classes of elliptic curves

over $\mathbb{F}_q$ by their trace [7, Theorem 4.1]; the chapter containing it is presented by its author as a rederivation of Deuring's results [8]. For *prime* q that classification admits every integer N with $|N-(q+1)| \le 2\sqrt{q}$ as the order of some elliptic curve over $\mathbb{F}_q$, whereas at a proper prime power part of the Hasse interval can be inadmissible: at $q=25$ the value $N=26$ is not an order, at $q=49$ neither 43 nor 57 is, and at $q=128$ only 25 of the 45 integers of the interval are. That is suggestive of the dichotomy in Theorems 5.1 and 5.2, but it is no more than suggestive, and it is not an explanation. The mismatch is already visible at the two smallest proper prime powers: at $q=4$ and at $q=9$ Waterhouse's classification admits *every* integer of the Hasse interval, and yet the equality of Theorem 5.1 fails at both — at $q=4$ the value $N=9$ is admissible and is nevertheless not a realised reduced orbit length. The gap is presumably that the fibres of the integral of motion form a pencil rather than ranging over all curves. Comparing the multiset of fibre point counts with the realised spectrum is the obvious next computation.

6. Past the published range

The verification of [1] covers the prime powers $2 \le q \le 499$. The next prime power is 503.

Theorem 6.1. *Conjectures A and B hold for every one of the* 3 534 638 *orbits of* (1) *over* $\mathbb{F}_{503}$*: for every* $s \in \mathbb{F}_{503}^{\times}$ *and every coset of* $\langle s\rangle$ *in* $\mathbb{F}_{503}^{\times}$*. The largest reduced orbit length is* 548 *and the smallest is* 1*. Moreover* $H(503) = 548$*, so the maximum is again the largest integer strictly below the Hasse bound.*

Proof sketch. Exhaustive computation: $6.40 \times 10^{10} = (503^2-1)^2$ evolution steps. The sweep was split into six equal ranges of s — the per-s cost $(q+1)^2(q-1) = 1.275 \times 10^8$ steps is uniform in s, so equal ranges are equal work — each range evaluated separately, and the six results recombined by a purely symbolic step: the combination rule takes the conjunction of the six Booleans, the maximum of the six maxima and the minimum of the six minima, and evaluating it on the six results is kernel arithmetic that re-runs no sweep. Each of the six asserts, over its range of s, that the field tables audit correctly, that the reduced lengths from each $X_{t_0,s}$ sum to $(q+1)^2$, that every reduced length satisfies both conjectures, and that the extreme lengths over that range are 548 and 1. As in Theorem 4.1, nothing is sampled. The value $H(503) = 548 = 504 + 44$ is arithmetic ($44^2 = 1936 < 2012$, $45^2 = 2025 > 2012$). □

Theorem 6.2. *Let* $s \in \{1, 2, \dots, 12\} \subseteq \mathbb{F}_{1009}^{\times}$*. Conjectures A and B hold for every one of the* 5 756 256 *orbits of* (1) *over* $\mathbb{F}_{1009}$ *with that* s *and* t_0 *running over every coset of* $\langle s\rangle$*; the largest reduced orbit length is* $1073 = H(1009)$ *and the smallest is* 1*. Here* $M_{1009} = 8$*.*

Proof sketch. Exhaustive computation over the stated twelve values of s: 1.23×10^{10} evolution steps, of the same shape as Theorem 6.1 and with the same fused completeness check. By Lemma 2.3 the statement is complete in s: for each of the twelve values, *every* orbit of (1) over $\mathbb{F}_{1009}$ with that s is accounted for. A complete sweep over all 1008 values of s is 1.04×10^{12} steps and was not run. The twelve orders of s are $1, 504, 168, 252, 504, 252, 252, 168, 84, 252, 1008, 504$, six distinct divisors of 1008, and include $r=1$ (the autonomous case) and $r = q-1$ (a primitive root, $s=11$). □

The interest of $q=1009$ is not only its size. The deepest bin structure printed in [1] is $M_{499} = 6$; at $q=1009$ there are eight bins, so Conjecture B is being tested two bins deeper than anywhere in the source, and the largest length found is the largest integer of B_1.

Remark 6.3 (Unverified computations, recorded as such). Every reduced orbit length, bin endpoint and extremal value appearing in a theorem, proposition or corollary of this paper is machine-checked. Two kinds of number in the statements above are not, and should be read as bookkeeping rather than as part of the assertion: the orbit counts (3 534 638 at $q=503$, 5 756 256 at $q=1009$, 3 222 405 and 3 327 974 over the band $q \le 131$) and the evolution-step counts, neither of which the verified Booleans return. What the verification does return, for every cell, is the completeness identity of

Lemma 2.3 — that the reduced lengths found in each $X_{t_0,s}$ sum to $(q+1)^2$ — which is what makes the orbit counts complete rather than merely large.

The following is not machine-checked at all. A reference implementation in C, written independently of the formal development and used to price the sweeps and to predict every value before it was stated, reproduces all of the above, and in addition reports: a complete sweep at $q = 199$ and at $q = 509$, the latter with 4 929 866 orbits, maximum reduced length $555 = H(509)$ and no violation of either conjecture; and the equality of Theorem 5.1 at $q = 199, 503, 509$ and at $q = 1009$ restricted to $s \le 12$. Those cells are stated only here, are part of no theorem, and carry no verification.

7. Reproduction of the published data, and negative controls

Everything above rests on an implementation of Algorithms 1 and 3 of [1] written from the paper. Before anything was claimed, that implementation was made to reproduce every number [1] prints.

Theorem 7.1. *The implementation used for all the results above reproduces exactly the following data of* [1].

(i) ([1, §2.2.1], $q = 2$) *Two orbits, of lengths* 5 *and* 4*; with* $s = t = 1$ *and* $r = 1$ *the reduced lengths are* 4 *and* 5*, one orbit each.*
(ii) ([1, §2.2.1], $q = 3$, $s = 2$, $t = 1$) *Three orbits, of lengths* $8, 10, 14$*, i.e. reduced lengths* $4, 5, 7$.
(iii) ([1, §2.2.1], $q = 4 = \mathbb{F}_2[a]/(a^2 + a + 1)$, $s = a$, $t = 1$) *Five orbits, two of length* 12*, one of* 15*, two of* 18*; reduced lengths* $4, 4, 5, 6, 6$.
(iv) ([1, §2.3], $q = 5$) *The three frequency lists* L_1, L_2, L_4*, entry for entry.*
(v) ([1, §2.4], $q = 499$, $s = 140$, $t = 1$) *The absolute bin frequencies* 113831*,* 54446*,* 13551*,* 19140*,* 6935*,* 42097*, totalling* $250000 = (q+1)^2$*; and the six bins of Proposition 3.3.*

Proof sketch. Direct evaluation, one exhaustive decomposition per data point. Item (iii) is the only one of the five that exercises the extension-field arithmetic against a number printed in the source rather than against the implementation itself: $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+X+1)$ with $s = a$ of multiplicative order 3. The presentation of every $\mathbb{F}_{p^n}$ used anywhere in this paper is audited by re-deriving the entire multiplication table from the defining polynomial and comparing it with the tables actually used, and by checking every tabulated inverse, so a reducible or mistyped defining polynomial cannot pass unnoticed. □

The verification of Theorem 4.1 together with Theorem 4.2 covers all 45 prime powers $q \le 131$ and 3 327 974 orbits. That range lies inside the range $2 \le q \le 499$ already verified with Magma in [1], so it adds no new cell; what it adds is a second, independent implementation agreeing with the first, which is what licenses Theorems 6.1 and 6.2 outside the published range.

Proposition 7.2. (i) (A weaker bound is false.) *The term* $2\sqrt{q}$ *in Conjecture A cannot be dropped: over* $\mathbb{F}_3$ *there is an orbit of reduced length* $7 > q + 1 = 4$*, and over* $\mathbb{F}_7$ *one of reduced length* $13 > 8$.
(ii) (A stronger sharpness statement is false.) *"The bound is attained at every prime power" is refuted by Theorem 4.2: the maximum at* $q = 128$ *is* 150 *and* $H(128) = 151$.
(iii) (The bins are strictly stronger than the bound.) *At* $q = 131$ *the value* 78 *satisfies* (4) — *it is below* $H(131) = 154$ — *but lies in no bin, the three bins being* $[110, 154]$, $[55, 77]$ *and* $[1, 51]$. *So Conjecture B is not a restatement of Conjecture A, and Theorem 4.1 asserts in particular that* 78 *is not a reduced orbit length at* $q = 131$.
(iv) (Not vacuous.) *At* $q = 131$ *the complete sweep returns largest reduced length* $154 = H(131)$ *and smallest* 1*, with the completeness identity of Lemma 2.3 holding for every* (s, t_0)*; and* 154 *does lie in* B_1.

Proof sketch. Items (i) and (iv) are readings of complete sweeps already run; (ii) is Theorem 4.2; (iii) is evaluation of (4) and (5) at $q = 131$, $L = 78$, together with the bin endpoints. Every value was computed before it was written into a statement. The half of (i) concerning $\mathbb{F}_7$ is verified without appeal to compiled code (Section 8). □

8. Verification

Every theorem, proposition and corollary above has been formally verified in Lean 4 [10] (toolchain `v4.32.0`), the statements involving real square roots against *Mathlib* [11]; the development contains no `sorry`, and the repository reference is to be added at submission. Five items are the exceptions, each proved here by hand either from a verified statement or from elementary algebra, and each flagged where it occurs: Lemma 2.3; the monotonicity of mq recorded after Proposition 3.3; Proposition 3.4; Corollary 5.3; and Remark 6.3, which is a report of unverified computation and is labelled as such. Lemma 2.3 deserves a word: it is the mathematical justification for the shape of every computation below, and the completeness identity it predicts — that the reduced lengths obtained from one $X_{t_0,s}$ sum to $(q+1)^2$ — is itself re-checked inside every computation, for every (s, t_0), so a failure of the lemma would show up as a failed sweep rather than as a silent gap.

The division of labour within the verified part is as follows. Propositions 2.2, 3.1 and 3.2 are proved without any computation — the first for an arbitrary field, with no finiteness hypothesis — and use no axioms beyond `propext`, `Classical.choice` and `Quot.sound`. The evaluations of H and of mq, including $H(503) = 548$, $H(1009) = 1073$ and Proposition 3.3's seven values of mq, are integer arithmetic that Lean's kernel performs itself and depend on no axioms at all. What is delegated to compiled evaluation (Lean's `native_decide`) is exactly the finite searches, and each is a single Boolean that fuses the field-table audit, the completeness identity of Lemma 2.3 for every (s, t_0), the two conjectures for every reduced length found, and the extremal values: one such Boolean per prime power for Theorems 4.1 and 4.2, one per prime for Theorem 5.1, one per range of s for Theorems 6.1 and 6.2, and one per item for Theorem 7.1 and Proposition 7.2 — several items of the latter being pure integer arithmetic the kernel does itself. Compiled evaluation is the standard trade: it puts Lean's compiler and runtime into the trusted base. Two things limit that exposure. First, the $q = 503$ sweep of Theorem 6.1 is split into six evaluations and recombined symbolically, and the resulting theorem depends on exactly the six evaluation axioms and nothing further, which is the check that the recombination re-evaluates nothing. Second, Proposition 4.3 and the $\mathbb{F}_7$ half of Proposition 7.2(i) — the whole band $q \le 7$ — are discharged *inside Lean's kernel*, with no compiled code and no evaluation axiom at all, by a second implementation that shares with the first only the arithmetic predicates (4) and (5): it uses modular arithmetic where the first uses logarithm tables, computes inverses by repeated squaring where the first tabulates them, and walks every one of the $(q+1)^2$ states as a start point where the first tracks which states have been visited. The separate statement that the two implementations return the same four maxima has an array-engine value on one side and so carries the compiled evaluation axioms for that side only.

The certified development costs about 1.2 hours of CPU in total, of which the $q = 503$ sweep is 56 minutes and the $q = 1009$ sweep 10; the kernel evaluation of the band $q \le 7$ is the most memory-hungry of the evaluations, at about 4.2 gigabytes. Finally, two limits of what the verification means. The evolution of Definition 2.1, used in Proposition 2.2 over an arbitrary field, and the implementation used in the sweeps are transcriptions of one another; no proof links them, and Theorem 7.1 is the calibration that stands in for one. And the identification of the integer $\mathrm{mq}(q)$ with the ceiling of [1, Conjecture 1.2.B], Proposition 3.4, is elementary but was done by hand, not formally.

References

[1] N. Joshi and P. Roffelsen, *Arithmetic dynamics of a discrete Painlevé equation*, J. Phys. A: Math. Theor. **59** (2026), no. 19, 195201, doi:10.1088/1751-8121/ae67bf; e-print arXiv:2508.18578 [nlin.SI], v1 (26 August 2025), v2 (16 January 2026), doi:10.48550/arXiv.2508.18578. All definition, algorithm, section and conjecture numbers quoted above are those of arXiv version 2, read off a compilation of its e-print source; the conjectures are unchanged from v1.

[2] N. Joshi and P. Roffelsen, *On integrals of non-autonomous dynamical systems in finite characteristic*, arXiv:2602.09298 [nlin.SI], v1 (10 February 2026), doi:10.48550/arXiv.2602.09298.

[3] N. Joshi, T. Lasic Latimer and P. Roffelsen, *On difference-differential Lax pairs and integrals of Painlevé equations in finite characteristic*, arXiv:2607.06980 [nlin.SI], v1 (8 July 2026), doi:10.48550/arXiv.2607.06980.

[4] P. Roffelsen, *Orbit data of q-difference Painlevé one over finite fields* (dataset), SeS Repository, The University of Sydney, 2025, doi:10.25910/sk02-0f22. The Magma orbit data for $2 \leq q \leq 499$ cited by [1]; "SeS Repository" is [1]'s own name for it.

[5] H. Sakai, *Rational surfaces associated with affine root systems and geometry of the Painlevé equations*, Comm. Math. Phys. **220** (2001), no. 1, 165–229, doi:10.1007/s002200100446.

[6] M. Murata, *Lax forms of the q-Painlevé equations*, J. Phys. A: Math. Theor. **42** (2009), no. 11, 115201, doi:10.1088/1751-8113/42/11/115201.

[7] W. C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) **2** (1969), no. 4, 521–560, doi:10.24033/asens.1183. The classification used above is Theorem 4.1, in Chapter 4 (*Elliptic Curves*); the author's introduction describes that chapter as applying his theory to rederive the classical results of Deuring [8] on elliptic curves, and says the same at the head of the chapter itself.

[8] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272, doi:10.1007/BF02940746.

[9] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system I: the user language*, J. Symbolic Comput. **24** (1997), no. 3–4, 235–265, doi:10.1006/jsco.1996.0125. [1] reports using Magma V2.28-23.

[10] L. de Moura and S. Ullrich, *The Lean 4 theorem prover and programming language*, in: Automated Deduction — CADE 28, Lecture Notes in Computer Science **12699**, Springer, 2021, 625–635, doi:10.1007/978-3-030-79876-5_37.

[11] The mathlib Community, *The Lean mathematical library*, in: Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020), ACM, 2020, 367–381, doi:10.1145/3372885.3373824.