hexagon:2611.00883v1

Total-Collapse Primes of Polynomial Maps over $\mathbb{F}_p$: Eighteen Families and Two Related Sequences

Igor M. Zhuk
Independent Researcher
igor.m.zhuk@gmail.com
ORCID: 0009-0003-1670-8388

Abstract

For a polynomial map $T : \mathbb{F}_p \to \mathbb{F}_p$ and a nonempty set $A \subseteq \mathbb{F}_p$, a prime p is a *total-collapse prime* for (T, A) if every forward orbit in $\mathbb{F}_p$ eventually enters A; when A is T-invariant and periodic, every directed cycle of T on $\mathbb{F}_p$ lies in A. Extending Vasiga and Shallit's study of $x^2 - 2 \pmod p$, we study 18 polynomial families over $\mathbb{F}_p$: seven odd cubics $\mathcal{K}_n(u) = (u^3-(n^2+n+1)u)/(n(n+1))$ (A401667), seven Chebyshev–Dickson squares $V_m(x)^2$ (A401173; OEIS drafts A399326, A402659), three Hilbert class field and octic maps (A401959, A402158; OEIS draft A399684), and $x^2(x-2)^2$. Using dynatomic factorizations, Stickelberger's parity theorem, the dihedral group D_7 for $\mathbb{Q}(\sqrt{-251})$, and Dickson's permutation criterion, we prove necessary conditions for total collapse in each family. Along the cubic ladder $\mathcal{K}_n$ (A398745), whenever $n^2 + (n+1)^2 = c^2$ ($n \in$ A001652, $c \in$ A001653), total collapse for $p > n + 1$ requires c prime and $p = c$. We also study sums of n-bit one-zero-block primes (A401666) and certify prime tables across all 20 sequences.

2020 Mathematics Subject Classification: Primary 11B83; Secondary 37P05, 11T06, 11R37.
Keywords: arithmetic dynamics, finite field, functional graph, Chebyshev polynomial, Dickson polynomial, Hilbert class field, Pell equation, integer sequence.

1 Introduction and general lemmas

Functional graphs of low-degree polynomials over finite fields $\mathbb{F}_p$ have been studied by Vasiga and Shallit [12] for $x \mapsto x^2$ and $x \mapsto x^2 - 2$, by Silverman [10] in arithmetic dynamics, and by Konyagin et al. [6] for general cycle bounds. For the squaring map $x \mapsto x^2 \pmod p$ with target $\{0, 1\}$, every nonzero element reaches 1 if and only if $p - 1$ is a power of 2, recovering $p = 2$ together with the Fermat primes (A019434). Replacing x^2 by the squared Chebyshev–Dickson map $T(x) = (x^2 - 2)^2 \pmod p$ with singleton target $\{1\}$ yields a sparse

prime sequence (A401173: $3, 5, 37, 59, 61, 109, 359, 5507, 2117573, \ldots$) constrained by 2-adic preimage trees and cubic Hilbert class field obstructions [13].

Throughout this paper, p denotes a prime, $\left(\frac{a}{p}\right)$ denotes the Legendre symbol for odd p, and $V_m \in \mathbb{Z}[x]$ denotes the monic Chebyshev–Dickson polynomial of the first kind defined by $V_m(t+t^{-1}) = t^m + t^{-m}$, with $V_0(x) = 2$, $V_1(x) = x$, and $V_m(x) = xV_{m-1}(x) - V_{m-2}(x)$ [7]. For the indices used below,

$$V_2(x) = x^2 - 2, \qquad V_3(x) = x(x^2 - 3), \qquad V_5(x) = x(x^4 - 5x^2 + 5),$$
$$V_6(x) = V_3(x)^2 - 2, \qquad V_7(x) = x(x^6 - 7x^4 + 14x^2 - 7), \qquad V_8(x) = V_2(V_2(V_2(x))),$$

and $V_9(x) = V_3(V_3(x))$.

Definition 1. Let $T \in \mathbb{Z}[1/B][x]$ for a nonzero integer B, let p be a prime with $p \nmid B$, and let $A \subseteq \mathbb{F}_p$ be nonempty. We say that p is a *total-collapse prime* for (T, A) if for every $x_0 \in \mathbb{F}_p$ there exists an integer $r \geq 1$ such that $T^{(r)}(x_0) \in A$.

Lemma 2. *Suppose $T(A) \subseteq A$ and every element of A is T-periodic. Then p is a total-collapse prime for (T, A) if and only if every directed cycle of the functional graph $(\mathbb{F}_p, T)$ is contained in A. Equivalently, $|\{x \in \mathbb{F}_p : T^{(p)}(x) \in A\}| = p$.*

Proof. Every forward orbit in the finite set $\mathbb{F}_p$ eventually enters a directed cycle. If all cycles lie in A, then every orbit enters A. Conversely, suppose there exists a cycle $C \not\subseteq A$. If $C \cap A = \emptyset$, points on C never enter A. If $C \cap A \neq \emptyset$, invariance $T(A) \subseteq A$ forces $C \subseteq A$, a contradiction. Since every orbit reaches its cycle in at most p steps and A is invariant, the condition is equivalent to $T^{(p)}(x) \in A$ for all $x \in \mathbb{F}_p$. □

Lemma 3. *Let $h, g : \mathbb{F}_p \to \mathbb{F}_p$ be maps, and set $T = g \circ h$ and $F = h \circ g$. Then h maps the periodic point set $\mathrm{Per}(T)$ bijectively onto $\mathrm{Per}(F)$, preserving cycle lengths and satisfying $h \circ T = F \circ h$. In particular, C is the unique cycle of T if and only if $h(C)$ is the unique cycle of F.*

Proof. From $h \circ T = F \circ h$ and $g \circ F = T \circ g$, the maps h and g send T-periodic points to F-periodic points and conversely. Restricted to $\mathrm{Per}(T)$ and $\mathrm{Per}(F)$, the compositions $g \circ h = T$ and $h \circ g = F$ are bijections, so $h|_{\mathrm{Per}(T)}$ is a cycle-preserving bijection conjugating T and F. □

Proposition 4. *For a singleton target $A = \{a\}$, Definition 1 holds if and only if the functional graph of T on $\mathbb{F}_p$ is connected and its unique cycle contains a. Allowing $r \geq 0$ in Definition 1 gives an equivalent condition.*

Proof. Taking $x_0 = a$ in Definition 1 with $r \geq 1$ shows that the forward orbit of a returns to a, so a lies on some cycle C_a. Any other cycle would be closed under T and disjoint from C_a, so its elements could never reach a; hence C_a is the unique cycle and the functional graph is connected. The converse is immediate. Allowing $r \geq 0$ does not admit any cycle disjoint from $\{a\}$, so a lies on every cycle and the same condition holds. □

2 The eighteen polynomial families

We study the 18 pairs (T, A) listed in Table 1, numbered as Families 00 through 17 to match the companion sequence cards and verification programs [14]. Here we set

$$P_{251}(z) = z^7 + 5z^6 + 6z^5 - 2z^4 - 4z^3 + 2z^2 + 9z - 1, \tag{1}$$

$$\mathcal{K}_n(u) = \frac{u^3 - A_n u}{B_n}, \qquad B_n = n(n+1), \qquad A_n = B_n + 1 = n^2 + n + 1. \tag{2}$$

Family	Polynomial map T	Target A	Admissible p	OEIS
00	$V_2(x)^2 = (x^2-2)^2$	$\{1\}$	all primes	A401173
01	$(z+2)(z^3+2z-1)+z$	$\{-2\}$	all primes	A401959
02	$V_3(x)^2 = x^2(x^2-3)^2$	$\{0\}$	all primes	A399326 (draft)
03	$(x^2-2)^4$	$\{1\}$	all primes	A399684 (draft)
04	$V_5(x)^2$	$\{0,1\}$	all primes	A402659 (draft)
05	$V_8(x)^2$	$\{1\}$	all primes	new
06	$V_9(x)^2$	$\{0\}$	all primes	new
07	$V_7(x)^2$	$\{0,1\}$	all primes	new
08	$(z+2)P_{251}(z)+z$	$\{-2\}$	all primes	A402158
09	$V_6(x)^2$	$\{4\}$	all primes	new
10	$D(x) = x^2(x-2)^2$	$\mathrm{Fix}(D)$	all primes	new
11	$\mathcal{K}_2(u) = (u^3-7u)/6$	$\{-1,0,1\}$	$p \geq 5$	A401667
12–17	$\mathcal{K}_n(u)$ for $n = 4,1,5,6,7,8$	$\{-1,0,1\}$	$p \geq 5$, $p \nmid B_n$	new

Table 1: The 18 polynomial families and their target sets over $\mathbb{F}_p$.

For every family except Family 09, the target set A is T-invariant and consists of periodic points, so Lemma 2 applies: $V_m(1)^2 = 1$ for $m \equiv \pm 2 \pmod 6$; $V_m(0) = 0$ for odd m; $V_m(1) = 1$ for $m \equiv \pm 1 \pmod 6$; $\mathcal{K}_n(0) = 0$ and $\mathcal{K}_n(\pm 1) = \mp 1$; and $T(-2) = -2$ for Families 01 and 08. For Family 09, Proposition 4 applies at $a = 4$.

Remark 5. For comparison, the degree-8 Chebyshev–Dickson square $V_4(x)^2 = ((x^2-2)^2-2)^2$ with target $\{1\}$ differs from both $(x^2-2)^2$ and $(x^2-2)^4$ and has collapsing primes $3, 5, 11, 13$ below $2 \cdot 10^4$. The projective indexing behind the $7+7+3+1$ partition of Families 00–17 is summarized in Section 6.

3 Necessary conditions for total collapse

3.1 The odd cubic ladder (Families 11–17)

Theorem 6. *For every integer $n \geq 1$, the following polynomial identities hold in $\mathbb{Z}[n, u]$:*

$$u^3 - A_n u - B_n = (u+1)(u+n)(u-n-1), \tag{3}$$
$$u^3 - A_n u + B_n = (u-1)(u-n)(u+n+1), \tag{4}$$
$$B_n^4\big(\mathcal{K}_n(\mathcal{K}_n(u)) - u\big) = u(u^2-1)\big(u^2 - D_{\text{fix}}\big)\big(u^4 - A_n u^2 + B_n^2\big), \tag{5}$$

where $D_{\text{fix}} = 2B_n + 1 = n^2 + (n+1)^2$ (A001844). Viewing the quartic factor in (5) as a quadratic in u^2, its discriminant factors as

$$A_n^2 - 4B_n^2 = D_2^+ D_2^-, \qquad D_2^+ = 3B_n + 1 = (n+1)^3 - n^3 \text{ (A003215)}, \qquad D_2^- = 1 - B_n.$$

Let $p \geq 5$ be a prime with $p \nmid B_n$. Then:

1. *If $\left(\frac{D_{\text{fix}}}{p}\right) = 1$, then $\pm\sqrt{D_{\text{fix}}} \in \mathbb{F}_p$ are fixed points of $\mathcal{K}_n$ outside $\{-1, 0, 1\}$, so p is not a total-collapse prime.*
2. *If $\left(\frac{D_2^+}{p}\right) = \left(\frac{D_2^-}{p}\right) = 1$, then the four roots $u = \frac{1}{2}(\pm\sqrt{D_2^+} \pm \sqrt{D_2^-}) \in \mathbb{F}_p$ form two 2-cycles outside $\{-1, 0, 1\}$, so p is not a total-collapse prime.*

Proof. Identities (3)–(5) hold by direct polynomial expansion. For part (1), $\sqrt{D_{\text{fix}}} \equiv \pm 1 \pmod p$ would imply $2B_n \equiv 0 \pmod p$, impossible since $p \geq 5$ and $p \nmid B_n$, while $\sqrt{D_{\text{fix}}} \equiv 0 \pmod p$ contradicts $\left(\frac{D_{\text{fix}}}{p}\right) = 1$.

For part (2), $u = 0$ is not a root of $u^4 - A_n u^2 + B_n^2$ because $p \nmid B_n$, and $u = \pm 1$ is a root only if $p \mid B_n(B_n - 1)$, that is, $p \mid D_2^-$. A common root with $u^2 - D_{\text{fix}}$ occurs only if $p \mid B_n(3B_n + 1) = B_n D_2^+$. Both divisibilities are excluded when $\left(\frac{D_2^+}{p}\right) = \left(\frac{D_2^-}{p}\right) = 1$. Since $4u^2 = (\sqrt{D_2^+} \pm \sqrt{D_2^-})^2$ in $\mathbb{F}_p$, all four roots lie in $\mathbb{F}_p$ and have exact period 2 outside $\{-1, 0, 1\}$. □

Corollary 7. *Among $1 \leq n \leq 8$, the discriminant $D_{\text{fix}} \in \{5, 13, 25, 41, 61, 85, 113, 145\}$ is an integer square only at $n = 3$ ($D_{\text{fix}} = 25$). For $n = 3$ and every prime $p > 5$, the residues $\pm 5 \bmod p$ are fixed points outside $\{-1, 0, 1\}$, whereas at $p = 5$ we have $\mathcal{K}_3(u) \equiv 3u^3 + u \pmod 5$, sending $\mathbb{F}_5$ onto $\{-1, 0, 1\}$ in one step. Thus $p = 5$ is the unique total-collapse prime for $\mathcal{K}_3$.*

3.2 Hilbert class field barriers (Families 00, 01, 08)

Theorem 8. *The following fixed-point obstructions hold:*

1. (Family 00, A401173.) *One has* $T(x) - x = (x-1)f(x)$, *where* $f(x) = x^3 + x^2 - 3x - 4$ *satisfies* $\operatorname{disc}(f) = -83$ *and* $f(1) = -5$. *If* $p > 5$, $p \neq 83$, *and* $\left(\frac{-83}{p}\right) = -1$, *then* $f \bmod p$ *has a unique linear factor, giving a fixed point* $x_0 \neq 1$ *in* $\mathbb{F}_p$, *so* p *is not a total-collapse prime. At* $p = 83$, $f(x) \equiv (x-44)^2(x-77) \pmod{83}$.

2. (Family 01, A401959.) *One has* $T(z) - z = (z+2)P_{59}(z)$, *where* $P_{59}(z) = z^3 + 2z - 1$ *satisfies* $\operatorname{disc}(P_{59}) = -59$ *and* $P_{59}(-2) = -13$. *If* $p \notin \{2, 13, 59\}$ *and* $\left(\frac{-59}{p}\right) = -1$, *there exists a fixed point* $z_0 \neq -2$ *in* $\mathbb{F}_p$. *At* $p = 59$, $P_{59}(z) \equiv (z-45)^2(z-28) \pmod{59}$.

3. (Family 08, A402158.) *One has* $T(z) - z = (z+2)P_{251}(z)$, *where* $\operatorname{disc}(P_{251}) = -2^{10} \cdot 251^3$, $P_{251}(-2) = -11$, *and the splitting field of* P_{251} *is the Hilbert class field* H *of* $\mathbb{Q}(\sqrt{-251})$ *with* $\operatorname{Gal}(H/\mathbb{Q}) \cong D_7$, *as computed via Ramanujan class invariants by Berndt and Chan [1] and Konstantinou and Kontogeorgis [5]; see also Cox [2]. If* $p \notin \{2, 251\}$ *and* $\left(\frac{-251}{p}\right) = -1$, *the Frobenius automorphism at* p *is a reflection in* D_7 *of cycle type* $(1)(2)(2)(2)$, *so* $P_{251} \bmod p$ *has a unique root in* $\mathbb{F}_p$. *For* $p \neq 11$ *this root differs from* -2, *preventing total collapse.*

Proof. All factorizations and discriminants follow by direct calculation. By Stickelberger's parity theorem [11], for any prime $p \nmid 2\operatorname{disc}(g)$ of a squarefree polynomial g of degree d, one has $\left(\frac{\operatorname{disc}(g)}{p}\right) = (-1)^{d-r}$, where r is the number of irreducible factors of $g \bmod p$. For $d = 3$ and Legendre symbol -1, we get $r = 2$, forcing the degree partition $1+2$ and hence a unique root in $\mathbb{F}_p$.

In part (3), any odd prime inert in $\mathbb{Q}(\sqrt{-251})$ has Frobenius automorphism lying in the coset $D_7 \setminus C_7$, which consists of the seven reflections. Every reflection of a regular heptagon fixes one vertex and swaps the remaining six in three pairs; by Dedekind's theorem (for $p \neq 2$, since the polynomial index is 2^5), $P_{251} \bmod p$ factors with degree pattern $(1, 2, 2, 2)$, while $p = 2$ is excluded directly since $T(0) \equiv 0 \pmod 2$ and $T(1) \equiv 1 \pmod 2$ whereas $-2 \equiv 0 \pmod 2$ does not absorb 1. □

Corollary 9. *The imaginary quadratic fields of fundamental discriminants* $D = -83$, -59, *and* -251 *have prime class numbers* 3, 3, *and* 7, *respectively, and the Galois closures of* f, P_{59}, *and* P_{251} *coincide with their Hilbert class fields [2]. Because the class group is cyclic of prime order in each case, an unramified prime* p *splitting in* $\mathbb{Q}(\sqrt{D})$ *keeps the class polynomial irreducible modulo* p *if and only if* p *is represented by a non-principal binary quadratic form of discriminant* D, *while at the ramified primes* $p \in \{83, 59, 251\}$ *each polynomial has roots in* $\mathbb{F}_p$ *distinct from the target and* p *is represented only by the principal form. Consequently:*

1. *For Family* 00 *(A401173) and* $p > 5$, $x = 1$ *is the unique fixed point in* $\mathbb{F}_p$ *if and only if* $p = 3x^2 + xy + 7y^2$ *for integers* x, y.

2. *For Family* 01 *(*A401959*) and* $p > 13$, $z = -2$ *is the unique fixed point in* $\mathbb{F}_p$ *if and only if* $p = 3x^2 + xy + 5y^2$.

3. *For Family* 08 *(*A402158*) and* $p > 11$, $z = -2$ *is the unique fixed point in* $\mathbb{F}_p$ *if and only if* p *is represented by one of the non-principal forms* $3x^2 + xy + 21y^2$, $7x^2 + xy + 9y^2$, *or* $5x^2 + 3xy + 13y^2$.

In addition, the substitution $z = x^2 - 3$ *maps the roots of* $f(x) = x^3 + x^2 - 3x - 4$ *to the roots of* $z^3 + 2z^2 + 2z - 1$.

3.3 Chebyshev–Dickson squares and permutation barriers

Theorem 10. *The following preimage barriers hold:*

1. (Families 02 and 06; draft A399326.) *If* $p > 3$ *satisfies* $\left(\frac{3}{p}\right) = -1$, *then* $V_3(x) \equiv 0 \pmod p$ *holds only at* $x = 0$, *so the preimage basin of* 0 *under* V_3^2 *and* V_9^2 *reduces to* $\{0\}$. *Hence every odd prime in Families* 02 *and* 06 *satisfies* $p \equiv \pm 1 \pmod{12}$.

2. (Families 00, 03, and 05; A401173, draft A399684.) *If* $p \equiv 7 \pmod{12}$, *so that* $\left(\frac{-1}{p}\right) = \left(\frac{3}{p}\right) = -1$, *then* $(u^2 - 2)^2 \equiv 1 \pmod p$ *implies* $u^2 \in \{1, 3\}$, *whence* $u \equiv \pm 1 \pmod p$, *while* -1 *has no square or fourth-power root in* $\mathbb{F}_p$. *By induction along* V_2, *the backward basin of* 1 *equals* $\{1, -1\}$ *of size* $2 < p$, *excluding* p.

3. (Dickson permutation barrier, Families 04 and 07; draft A402659.) *Let* $m \in \{5, 7\}$, $p > m$, *and* $\gcd(m, p^2 - 1) = 1$. *By Dickson's theorem [3] (see also Lidl and Niederreiter [7, Ch. 7]),* V_m *permutes* $\mathbb{F}_p$, *with* $V_m(0) = 0$ *and* $V_m(\pm 1) = \pm 1$. *Thus* $T^{-1}(0) = \{0\}$ *and* $T^{-1}(1) = \{\pm 1\}$ *for* $T = V_m^2$. *If also* $p \equiv 3 \pmod 4$, *then* -1 *has no preimage under* T, *so the backward basin of* $\{0, 1\}$ *is* $\{0, 1, -1\}$ *of size* $3 < p$, *excluding* p.

Proof. Parts (1) and (2) follow from quadratic reciprocity and preimage inspection. In part (3), since V_m is a bijection on $\mathbb{F}_p$ fixing $0, 1, -1$, the congruence $V_m(x)^2 \equiv 0 \pmod p$ has only the solution $x = 0$, while $V_m(x)^2 \equiv 1 \pmod p$ means $V_m(x) \equiv \pm 1 \pmod p$, giving $x \equiv \pm 1 \pmod p$. When $p \equiv 3 \pmod 4$, -1 is a quadratic nonresidue, so $V_m(x)^2 \equiv -1 \pmod p$ has no solution in $\mathbb{F}_p$, closing the preimage tree at $\{0, 1, -1\}$. □

Proposition 11. *By Lemma 3, Family* 00 *(*A401173*) is equivalent to total collapse of* $u \mapsto u^4 - 2$ *to* -1; *Family* 03 *(draft* A399684*) is equivalent to total collapse of* $u \mapsto u^8 - 2$ *to* -1 *(requiring in particular that* $(u^8 - u - 2)/(u + 1) = u^7 - u^6 + u^5 - u^4 + u^3 - u^2 + u - 2$, *of discriminant* -26522311, *have no root in* $\mathbb{F}_p$ *for* $p > 3$*); and Family* 05 *is equivalent to total collapse of* $u \mapsto V_8(u^2)$ *to* -1.

For Family 09, $T_6(0) = T_6(\pm 1) = T_6(\pm 2) = 4$, *and* 4 *is fixed if and only if* $p \mid V_6(4)^2 - 4 = 2^6 \cdot 3^3 \cdot 5^2 \cdot 13^2$. *For Family* 10, $D(x) - x = x(x - 1)(x^2 - 3x + 1)$ *and* $D(2 - x) = D(x)$; *for odd* p, $\mathrm{Fix}(D) = \{0, 1\}$ *when* $\left(\frac{5}{p}\right) = -1$ *and* $\{0, 1, (3 \pm \sqrt{5})/2\}$ *when* $\left(\frac{5}{p}\right) \in \{0, 1\}$, *and* D *is*

the diagonal restriction $x = y$ of the coordinatewise square $(x, y) \mapsto ((x^2 - 2y)^2, (y^2 - 2x)^2)$ of the SL_3 power-trace map $(\operatorname{tr} A, \operatorname{tr} A^{-1}) \mapsto (\operatorname{tr} A^2, \operatorname{tr} A^{-2})$.

4 Two related integer sequences (A398745 and A401666)

4.1 Least collapsing prime along the cubic ladder (A398745)

Definition 12. For each integer $n \geq 1$, let $a(n)$ (A398745) denote the least prime $p \geq 5$ with $p > n + 1$ that is a total-collapse prime for $\mathcal{K}_n$ with target $\{-1, 0, 1\}$, or $a(n) = 0$ if no such prime exists.

The condition $p > n + 1$ prevents modular aliasing, since $\mathcal{K}_n \bmod p$ depends only on $n \bmod p$; for instance, $\mathcal{K}_{119} \equiv \mathcal{K}_2 \pmod{13}$ where 13 collapses $\mathcal{K}_2$. The initial terms of A398745 for $1 \leq n \leq 30$ are

$$5, 5, 5, 7, 7, 11, 19, 19, 41, 13, 13, 17, 127, 19, 23,$$
$$19, 23, 31, 31, 0, 23, 31, 53, 29, 37, 89, 89, 31, 41, 67,$$

with $a(13) = 127$ (A000668), $a(20) = 0$, $a(43) = 991$, and $a(45) = 8713$.

Theorem 13 (Pell–Pythagorean obstruction)**.** *Suppose $n \geq 1$ satisfies $n^2 + (n + 1)^2 = c^2$ with $c > 0$, so that n belongs to A001652 $((0, 3, 20, 119, 696, 4059, 23660, \ldots))$ and c belongs to A001653 $((1, 5, 29, 169, 985, 5741, 33461, \ldots))$; cf. A002315 and A086383). Then for every prime $p > n + 1$:*

1. *The residues $\pm c \bmod p$ are fixed points of $\mathcal{K}_n$.*
2. *One has $\pm c \in \{-1, 0, 1\} \pmod p$ if and only if c is prime and $p = c$, in which case $\mathcal{K}_n(u) \equiv u(1 - 2u^2) \pmod c$.*

Consequently, every Pell level $n \in$ A001652 with $n \geq 1$ admits at most finitely many total-collapse primes ($p \leq n + 1$, together with at most $p = c$ when c is prime); in A398745, $a(n) = 0$ whenever c is composite and $a(n) \in \{0, c\}$ whenever c is prime.

Proof. By Theorem 6, $D_{\mathrm{fix}} = c^2$ yields the integer fixed points $\pm c$. Every prime factor of $c^2 - 1 = 2n(n + 1)$ is at most $n + 1 < p$, so $p \nmid (c \mp 1)$. Moreover, $c < \sqrt{2}(n + 1) < 2(n + 1)$. Since c is odd, if c is composite then its least prime factor is at most $c/3 < n + 1 < p$ and its greatest prime factor is at most $c/3 < p$, so $p \nmid c$. If c is prime, $p \mid c$ holds if and only if $p = c$. Finally, $2B_n = c^2 - 1 \equiv -1 \pmod c$ gives $B_n^{-1} \equiv -2 \pmod c$ and $A_n = B_n + 1 \equiv 1/2 \pmod c$, whence $\mathcal{K}_n(u) \equiv -2(u^3 - u/2) \equiv u(1 - 2u^2) \pmod c$. □

Example 14. At $n = 3$ ($c = 5$), $a(3) = 5$. At $n = 20$ ($c = 29$), $\mathcal{K}_{20} \bmod 29$ has the 4-cycle $22 \to 12 \to 7 \to 17 \to 22$, so $a(20) = 0$. At $n = 119$ ($c = 169 = 13^2$) and $n = 696$ ($c = 985 = 5 \cdot 197$), c is composite, giving $a(119) = a(696) = 0$ unconditionally. At the prime

hypotenuses $c = 5741$ ($n = 4059$) and $c = 33461$ ($n = 23660$), direct evaluation exhibits cycles outside $\{-1, 0, 1\}$ (such as $1762 \to 3531 \to 3979 \to 2210 \to 1762 \pmod{5741}$), so $a(4059) = a(23660) = 0$. For the next three positive legs $n \in$ A001652, the hypotenuses $195025 = 5^2 \cdot 29 \cdot 269$, $1136689 = 137 \cdot 8297$, and $6625109 = 37 \cdot 179057$ are composite, giving $a(n) = 0$ as well.

Conjecture 15. In A398745, $a(n) = 0$ for all $n \in$ A001652 with $n > 3$.

4.2 Sums of binary one-zero-block primes (A401666)

Definition 16. For each integer $n \geq 2$, let $b(n)$ (A401666) denote the sum of all n-bit primes of the form $2^n - 1$ (A000668) or

$$B(n, k, s) = (2^n - 1) - 2^s(2^k - 1), \qquad 1 \leq k \leq n - 2, \qquad 1 \leq s \leq n - 1 - k,$$

namely the odd n-bit prime terms of A100724 (whose binary expansion consists of a single circular run of 1s and at most one internal block of 0s; the single-zero case $k = 1$ includes primes related to A014234).

The initial terms of A401666 for $2 \leq n \leq 17$ are

$$3, 12, 24, 119, 167, 657, 1895, 4563, 6687,$$
$$22176, 30913, 104134, 175320, 372369, 1203372, 2977563.$$

Proposition 17. *For $B(n, k, s) = (2^n - 1) - 2^s(2^k - 1)$:*

1. *If $n \geq 4$ is even and k is even, then $3 \mid B(n, k, s)$ and $B(n, k, s) \geq 2^{n-1} + 1 > 3$, so every prime summand of $b(n)$ for even $n \geq 4$ has odd zero-block length k.*

2. *If $n \geq 5$ is odd, k is odd, and s is even, then $3 \mid B(n, k, s)$ and $B(n, k, s) > 3$ is composite.*

Proof. Since $2 \equiv -1 \pmod 3$, one has $2^m - 1 \equiv 0 \pmod 3$ for even m and $2^m - 1 \equiv 1 \pmod 3$ for odd m. Both congruences follow directly, while $B(n, k, s) \geq B(n, n - 2, 1) = 2^{n-1} + 1 \geq 9 > 3$ for $n \geq 4$. □

5 Computational verification and prime tables

In the companion C verifier [14], exact membership of a candidate prime p is decided in two stages after applying the algebraic filters of Section 3:

1. *Certified rejection:* Brent's cycle-detection algorithm is run from deterministic starting residues with no step bound; exhibiting a directed cycle C disjoint from A ($C \cap A = \emptyset$) certifies that p is not a total-collapse prime.

2. *Certified acceptance:* An exhaustive three-color traversal of all p elements of $\mathbb{F}_p$ verifies that every directed cycle meets A ($C \cap A \neq \emptyset$, which by Lemma 2 and Proposition 4 is equivalent to total collapse across all 18 families, including Family 09 where at $p = 7$ the 2-cycle $0 \leftrightarrow 4$ passes through $A = \{4\}$).

The open verification archive [14] provides standalone Julia programs for all symbolic identities and full-graph self-tests ($p < 2 \cdot 10^4$) together with the multi-threaded C verifier reproducing the $p \leq 10^6$ scans. In Table 2, P_{exact} denotes the bound up to which every prime $p \leq P_{\text{exact}}$ was tested in extended exact runs with no step cap, establishing completeness of the listed terms up to P_{exact}. By contrast, P_{scan} denotes a larger interval screened by bounded-step orbit probes ($\approx 6\sqrt{p}$ to $8\sqrt{p}$ steps); above P_{exact}, completeness remains open because an unclosed long transient does not prove an extraneous cycle. All 223 entries in Table 2 with $p < 2 \cdot 10^9$ are certified by full-field three-color traversal of $\mathbb{F}_p$, and the eleventh term $p = 20900146669$ of Family 00 (A401173) is certified by exhaustive traversal of all $(p+1)/2 = 10450073335$ sign classes $\{x, -x\}$ using $T(-x) = T(x)$ [13].

Fam.	Known total-collapse primes	P_{exact}	P_{scan}
00	3, 5, 37, 59, 61, 109, 359, 5507, 2117573, 503734381, 20900146669	$3 \cdot 10^{10}$	$3 \cdot 10^{10}$
01	3, 13, 137, 761, 2719, 150083	10^8	$2 \cdot 10^9$
02	2, 13, 23, 83, 17929, 18121	10^8	$2 \cdot 10^9$
03	3, 5, 13, 23, 41, 22381, 45503, 3852347, 1801981681	10^8	$2 \cdot 10^9$
04	2, 3, 5, 31, 59, 61, 89, 2939, 4261, 11839, 14137859, 599999971	10^6	$2 \cdot 10^9$
05	3, 5, 13, 17, 23, 47, 71, 89, 193, 313, 863, 1103, 1777, 107183, 84814153, 342037921	10^6	$2 \cdot 10^9$
06	2, 11, 73, 1297, 6733, 7393, 658871, 1295447	10^6	$2 \cdot 10^9$
07	2, 3, 5, 43, 421, 1429, 6257, 49279, 1580503, 24107329	10^6	$5 \cdot 10^8$
08	3, 7, 17, 233, 1373, 1531, 5861, 27427, 52937, 125287	10^6	$5 \cdot 10^8$
09	2, 3, 5, 7, 11, 13, 17, 37, 47, 79, 131, 167, 241, 257, 129401, 390209, 4926997, 6719077, 23734297	10^6	$5 \cdot 10^8$
10	2, 3, 5, 7, 11, 23, 29, 31, 59, 181, 521, 1559, 2069, 5261, 6871, 9551, 19207, 1161371, 1574681, 1849721, 85268251	10^6	$5 \cdot 10^8$
11	5, 7, 13, 19, 31, 47, 59, 73, 151, 331, 401, 1943069, 83584483, 158450797, 1554906533	10^6	$2 \cdot 10^9$
12	7, 11, 17, 19, 29, 41, 53, 79, 191, 42979, 277829, 35718901	10^6	$2 \cdot 10^9$
13	5, 7, 13, 23, 83, 97, 383, 14239193, 82411573	10^6	$2 \cdot 10^9$
14	7, 17, 23, 37, 313, 8753, 72173, 2952797, 3516973, 8879231, 334677433	10^6	$2 \cdot 10^9$
15	5, 11, 17, 31, 41, 109, 127, 199, 719, 2731, 26317, 307067, 617579, 4348559, 4838117, 30282823, 42166321, 62371087	10^6	$2 \cdot 10^9$
16	5, 19, 23, 151, 1237, 11941, 761357, 6756377, 1105256599	10^6	$2 \cdot 10^9$
17	5, 7, 19, 23, 31, 41, 53, 61, 277, 593, 809, 911, 1489, 2053, 4943, 6301, 17393, 229139, 324119, 1262783, 2055551, 228229363	10^6	$2 \cdot 10^9$

Table 2: Known total-collapse primes across the 18 families.

Alongside exact total collapse, near-collapse primes occur where every element of $\mathbb{F}_p$ outside the preimage basins of one or two short cycles reaches A; for example, in Family 00

at $p = 150662749$, two cycles of lengths 3 and 5 have combined basin size 282, so the target basin has density exceeding $1 - 2 \cdot 10^{-6}$.

Question 18. Is any of the 18 prime sequences in Table 2 finite, or are all 18 infinite?

Among uniform random maps on a p-element set with a distinguished fixed point, the proportion having no other cycles equals $p^{p-2}/p^{p-1} = 1/p$ by Cayley's tree formula (see Flajolet and Odlyzko [4]), and $\sum_p 1/p$ diverges, suggesting a doubly logarithmic heuristic $O(\log \log X)$ for the prime count up to X (cf. Rosser and Schoenfeld [9]). Because low-degree polynomials have structured dynatomic factorizations rather than uniform random behavior, this heuristic is not a proof; along the general cubic ladder $\mathcal{K}_n$, finiteness is proved unconditionally at every Pell level $n \in$ A001652 with $n \geq 1$ (Corollary 7 and Theorem 13).

6 Projective indexing in $\mathrm{PG}(3, 2)$

We record the projective combinatorics behind the $18 = 7+7+3+1$ indexing of Families 00–17. Identify the 15 points of $\mathrm{PG}(3, 2)$ with the nonzero 4-bit integers $1, \ldots, 15$. Four-bit reversal stabilizes the central line $L_0 = \{2, 4, 6\}$ setwise ($2 \leftrightarrow 4$, $6 \mapsto 6$), and the three Fano planes in $\mathrm{PG}(3, 2)$ containing L_0 are

$$L_0 \cup \{1, 3, 5, 7\}, \qquad L_0 \cup \{8, 10, 12, 14\}, \qquad L_0 \cup \{9, 11, 13, 15\},$$

cut out by $b_3 = 0$, $b_0 = 0$, and $b_3 = b_0$. The cyclic group C_7 acts freely by bit-rotations on $\mathbb{F}_2^7 \setminus \{0, 127\}$, partitioning the 126 non-constant vectors into $126/7 = 18$ orbits distributed across Hamming weights $1, \ldots, 6$ as $1 + 3 + 5 + 5 + 3 + 1$. Indexing the 7 odd cubics $\mathcal{K}_n$ ($n \in \{1, 2, 4, 5, 6, 7, 8\}$, where $\sum_{n=1}^{8} B_n = 240$ and $\sum_{n=1}^{8} A_n = 248$) by the 7 points of $\mathrm{PG}(2, 2)$, the 7 Chebyshev–Dickson squares V_m^2 by its 7 lines, Families 01, 03, 08 by the 3 Fano planes through L_0, and Family 10 by the ambient space gives the 18-family catalog.

7 Summary of OEIS sequences

Published sequences in the On-Line Encyclopedia of Integer Sequences [8] introduced by this investigation are A398745, A401173, A401666, A401667, A401959, and A402158; three further sequences are currently under editorial review as OEIS drafts A399326, A399684, and A402659. Existing OEIS sequences referenced in the proofs are A000668, A001652, A001653, A001844, A002315, A003215, A014234, A019434, A086383, and A100724.

References

[1] B. C. Berndt and H. H. Chan, Ramanujan and the modular j-invariant, *Canad. Math. Bull.* **42** (1999), 427–440.

[2] D. A. Cox, *Primes of the Form $x^2 + ny^2$*, 2nd ed., Wiley, 2013.

[3] L. E. Dickson, The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, *Ann. of Math.* **11** (1896), 65–120.

[4] P. Flajolet and A. M. Odlyzko, Random mapping statistics, in *Advances in Cryptology – EUROCRYPT '89*, Lecture Notes in Comput. Sci., Vol. 434, Springer, 1990, pp. 329–354.

[5] E. Konstantinou and A. Kontogeorgis, Computing polynomials of the Ramanujan t_n class invariants, *Canad. Math. Bull.* **52** (2009), 583–597.

[6] S. V. Konyagin, F. Luca, B. Mans, L. Mathieson, M. Sha, and I. E. Shparlinski, Functional graphs of polynomials over finite fields, *J. Combin. Theory Ser. B* **116** (2016), 87–122.

[7] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Cambridge University Press, 1997.

[8] OEIS Foundation Inc., *The On-Line Encyclopedia of Integer Sequences*, published electronically at https://oeis.org, 2026.

[9] J. B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois J. Math.* **6** (1962), 64–94.

[10] J. H. Silverman, *The Arithmetic of Dynamical Systems*, Graduate Texts in Mathematics, Vol. 241, Springer, 2007.

[11] L. Stickelberger, Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper, in *Verhandlungen des Ersten Internationalen Mathematiker-Kongresses*, Zürich, 1897, pp. 182–193.

[12] T. Vasiga and J. Shallit, On the iteration of certain quadratic maps over GF(p), *Discrete Math.* **277** (2004), 219–240.

[13] I. M. Zhuk, Unital collapse primes in arithmetic dynamics: total backward-orbit collapse for $T(x) = (x^2-2)^2 \bmod p$, Galois stratification, and Fermat–totient asymptotics, Zenodo preprint, 2026, https://doi.org/10.5281/zenodo.23420627.

[14] I. M. Zhuk, Total-collapse primes of polynomial maps over GF(p): verification suite and sequence cards, Zenodo archive, 2026, https://doi.org/10.5281/zenodo.23856837; code at https://github.com/Nondual-Observer/total-collapse-primes-oeis.