

# THE GALOIS GROUP OF A SEXTIC MISIUREWICZ POLYNOMIAL AND THE DENSITY OF ITS ROOT COUNTS MODULO $p$

GÖKTUĞ OMAV

ABSTRACT. Let

$$H(x) = x^6 + 2x^5 + 2x^4 + 2x^3 + x^2 + 1$$

be the sextic polynomial that parametrizes the primitive  $(2, 3)$ -Misiurewicz points of the quadratic family  $f_c(z) = z^2 + c$ ; equivalently,  $H$  is the degree-six factor of  $a_5(c) - a_2(c)$  (where  $a_0 = 0$ ,  $a_{k+1} = a_k^2 + c$ ) remaining after the factors coming from smaller preperiod and period are removed. The number of roots of  $H$  modulo the  $n$ -th prime is recorded in Sloane's OEIS as sequence A399163. We prove that  $H$  is irreducible over  $\mathbb{Q}$ , has discriminant  $-2^6 \cdot 743$ , and that its Galois group  $G = \text{Gal}(H/\mathbb{Q})$ , in its action on the six roots, is the full symmetric group  $S_6$ ; the proof uses Frobenius cycle types at two small primes together with a primitivity argument. By the Chebotarev density theorem this determines the statistics of A399163 completely: the number of roots of  $H$  modulo  $p$  takes the values  $0, 1, 2, 3, 4, 6$  with exact densities

$$\frac{53}{144}, \frac{11}{30}, \frac{3}{16}, \frac{1}{18}, \frac{1}{48}, \frac{1}{720},$$

respectively, and it never takes the value 5. We compare these predictions with the published terms of A399163 and with an independent computation over the first 20,000 primes.

## 1. INTRODUCTION

For  $c \in \mathbb{C}$  let  $f_c(z) = z^2 + c$ , and let

$$a_0(c) = 0, \quad a_{k+1}(c) = a_k(c)^2 + c,$$

so that  $a_k(c) = f_c^{\circ k}(0)$  is the  $k$ -th iterate of the critical point of  $f_c$ . A parameter  $c$  is a *Misiurewicz point of type  $(m, k)$*  if the critical orbit is strictly preperiodic, landing on a cycle of exact period  $k$  after exactly  $m$  steps; see Milnor [3] for background on the dynamics of the quadratic family. Every  $(m, k)$ -Misiurewicz point is a root of  $a_{m+k}(c) - a_m(c)$ , together with parameters of smaller preperiod or of period properly dividing  $k$ ; removing these lower-order factors isolates a primitive polynomial for each pair  $(m, k)$ .

---

*Date:* September 18, 2026.

*2020 Mathematics Subject Classification.* 11R32, 11R45, 11R09.

*Key words and phrases.* Galois group, Chebotarev density theorem, Misiurewicz point, quadratic family, OEIS.

For  $(m, k) = (2, 3)$  this primitive polynomial is

$$H(x) = x^6 + 2x^5 + 2x^4 + 2x^3 + x^2 + 1. \quad (1)$$

It is obtained from the factorization

$$a_5(c) - a_2(c) = c^3(c+2)(c^3+2c^2+c+1)^2 H(c), \quad (2)$$

readily checked by expanding  $a_5(c) - a_2(c)$ , a polynomial of degree  $2^4 = 16$ . Thus  $\deg H = 16 - 3 - 1 - 6 = 6$ .

The number of roots of  $H$  modulo the  $n$ -th prime  $p_n$  is Sloane's sequence [5]

$$a(n) = \#\{x \bmod p_n : H(x) \equiv 0 \pmod{p_n}\}, \quad n = 1, 2, 3, \dots$$

At the time of writing, the published values through  $n = 88$  contain no value larger than 4 except for a single 4, and no 5 at all. We explain this behavior by determining the Galois group of  $H$  and then applying the Chebotarev density theorem.

**Theorem 1.1.**  *$H$  is irreducible over  $\mathbb{Q}$ , with*

$$\text{disc}(H) = -2^6 \cdot 743,$$

*and its Galois group, acting on the six roots of  $H$ , is the full symmetric group  $S_6$ . Consequently:*

- (i) *For every prime  $p$ , including  $p = 2, 743$ , the number of roots of  $H$  modulo  $p$  lies in  $\{0, 1, 2, 3, 4, 6\}$ ; it is never 5.*
- (ii) *The asymptotic density of primes  $p$  for which  $H$  has exactly  $k$  roots modulo  $p$  is*

$$\frac{53}{144}, \frac{11}{30}, \frac{3}{16}, \frac{1}{18}, \frac{1}{48}, 0, \frac{1}{720} \quad \text{for } k = 0, 1, 2, 3, 4, 5, 6, \text{ respectively.}$$

## 2. IRREDUCIBILITY AND RAMIFICATION

**Proposition 2.1.**  *$\text{disc}(H) = -2^6 \cdot 743$ , and 743 is prime.*

*Proof.* Using  $\text{disc}(H) = \text{Res}(H, H')/\text{lc}(H)$ , a symbolic computation with SymPy [2] gives  $\text{disc}(H) = -47552 = -2^6 \cdot 743$ . Trial division confirms that 743 is prime.  $\square$

**Proposition 2.2.**  *$H$  is irreducible over  $\mathbb{Q}$ .*

*Proof.* It suffices to show that  $H$  is irreducible modulo the prime 5, since 5 does not divide the leading coefficient. We use the standard finite-field criterion: a degree- $n$  polynomial  $f \in \mathbb{F}_p[x]$  is irreducible if and only if

$$x^{p^n} \equiv x \pmod{f},$$

$$\gcd(f(x), x^{p^{n/q}} - x) = 1 \text{ for every prime } q \mid n.$$

Indeed,  $x^{p^d} - x$  is the product of all monic irreducibles of degree dividing  $d$ , so the first condition forces every irreducible factor of  $f$  to have degree dividing  $n$ , while the second rules out a factor of degree dividing  $n/q$  for

each prime  $q \mid n$ ; together these force every irreducible factor to have degree exactly  $n$ , i.e.  $f$  itself is irreducible (this also shows  $f$  is squarefree, since  $x^{p^n} - x$  is).

For  $H$  modulo 5 we have  $n = 6$ , so  $q \in \{2, 3\}$  and  $n/q \in \{3, 2\}$ . Repeated squaring in  $\mathbb{F}_5[x]/(H)$  gives

$$\begin{aligned} x^{25} &\equiv x^5 + 2x^3 + 3x^2 + 4, & x^{125} &\equiv x^4 + 2x^3 + x^2 + 2x + 2 \pmod{H, 5}, \\ x^{5^6} &\equiv x \pmod{H, 5}. \end{aligned}$$

Moreover,  $\gcd(H, x^{25} - x) = 1$  and  $\gcd(H, x^{125} - x) = 1$  in  $\mathbb{F}_5[x]$ . Hence  $H$  is irreducible modulo 5, and therefore irreducible over  $\mathbb{Q}$  by Gauss's lemma.  $\square$

By Proposition 2.1, every rational prime ramified in the splitting field of  $H$  divides the discriminant, hence is among 2 and 743. Direct computation gives

$$\begin{aligned} H(x) &\equiv (x^3 + x + 1)^2 \pmod{2}, \\ H(x) &\equiv (x - 301)^2(x^2 + 84x + 98)(x^2 - 223x - 356) \pmod{743}. \end{aligned}$$

In both cases the displayed factors account for all degree six, and direct inspection shows that  $H$  has no distinct root modulo 2 and exactly one distinct root modulo 743. In particular, neither ramified prime produces five roots.

### 3. THE GALOIS GROUP

Since  $H$  is irreducible of degree 6, its Galois group  $G = \text{Gal}(H/\mathbb{Q})$ , acting on the six roots, is a transitive subgroup of  $S_6$ .

None of 3, 5, 7 divides  $\text{disc}(H)$ , so these primes are unramified. At an unramified prime, the cycle type of a Frobenius element is the multiset of degrees of the irreducible factors of the reduction of  $H$  modulo that prime.

Modulo 3,

$$H(x) \equiv (x - 1)(x^5 - x^3 + x^2 - x - 1) \pmod{3},$$

and the degree-five factor is irreducible over  $\mathbb{F}_3$ . Thus  $G$  contains an element  $\rho$  of cycle type  $(5, 1)$ .

Modulo 7,

$$H(x) \equiv (x + 2)(x^2 - 3x + 1)(x^3 + 3x^2 + 3x - 3) \pmod{7},$$

where the displayed quadratic and cubic factors are irreducible over  $\mathbb{F}_7$ . Thus  $G$  contains an element  $\pi$  of cycle type  $(3, 2, 1)$ .

**Lemma 3.1.** *A transitive subgroup of  $S_6$  containing a 5-cycle is primitive.*

*Proof.* Suppose that  $G \leq S_6$  is transitive and has a nontrivial block system. Since 6 has proper divisors 2 and 3, a nontrivial block has size 2 or 3. Let  $\rho$  be a 5-cycle, fixing a point  $f$ , and let  $B$  be the block containing  $f$ . Since  $\rho(B)$  is a block containing  $\rho(f) = f$ , we have  $\rho(B) = B$ . Hence  $B$  is a union

of  $\langle \rho \rangle$ -orbits. These orbits have sizes 1 and 5, so  $|B|$  can only be 1, 5, or 6, a contradiction. Thus  $G$  is primitive.  $\square$

By the lemma,  $G$  is primitive. Since  $\pi$  has cycle type  $(3, 2, 1)$ , its cube is a single transposition: the 3-cycle becomes the identity, while the 2-cycle remains unchanged (an involution raised to an odd power is itself). Thus  $\pi^3 \in G$  is a transposition.

**Lemma 3.2.** *A primitive subgroup  $G \leq S_n$  containing a transposition equals  $S_n$ .*

*Proof.* Let  $\Gamma$  be the graph on  $\{1, \dots, n\}$  whose edges are the pairs  $\{i, j\}$  for which  $(ij) \in G$ . The hypothesis gives at least one edge. Conjugation by  $G$  preserves the set of edges (since  $g(ij)g^{-1} = (g(i)g(j))$ ), so  $G$  permutes the connected components of  $\Gamma$ . Since  $G$  is transitive, all components have the same size, and the components form a  $G$ -invariant block system. Primitivity therefore forces the component size to be 1 or  $n$ . Because  $\Gamma$  has an edge, it is connected.

It remains to note that the edge-transpositions of a connected graph on  $n$  vertices generate  $S_n$ . By induction on  $n$ : a spanning tree of  $\Gamma$  has a leaf edge  $(uv)$ , and the remaining edges span a connected graph on the other  $n-1$  vertices, which by induction generate  $\text{Sym}(\{1, \dots, n\} \setminus \{v\})$ ; adjoining  $(uv)$  gives a transitive subgroup of  $S_n$  whose stabilizer of  $v$  already contains this full symmetric group on  $n-1$  points, hence has order at least  $n \cdot (n-1)! = n!$ , so it equals  $S_n$ . Hence  $S_n \leq G$ , and therefore  $G = S_n$ .  $\square$

Applying the second lemma to the transposition  $\pi^3$  gives  $G = S_6$ . As an independent computational check, SymPy's Galois-group routine [2] also returns a group of order 720 for  $H$ ; further small primes, such as  $p = 29$ , where  $H$  has the factorization pattern  $(1, 1, 4)$  matching the 2 roots recorded in the OEIS example for  $p_{10} = 29$ , offer additional confirmation.

#### 4. THE CHEBOTAREV DENSITY THEOREM AND THE DENSITY FORMULA

We use the following standard form of Chebotarev's density theorem; see Lenstra–Stevenhagen [1] or Neukirch [4].

**Theorem 4.1** (Chebotarev). *Let  $f \in \mathbb{Z}[x]$  be monic of degree  $n$  with Galois group  $G \leq S_n$  acting on its roots, and let  $C \subseteq G$  be a union of conjugacy classes. Then the set of primes  $p$  unramified in the splitting field of  $f$  for which the Frobenius element at  $p$  lies in  $C$  has density  $|C|/|G|$ . Moreover, for such  $p$ , the cycle type of Frobenius equals the multiset of degrees of the irreducible factors of  $f$  modulo  $p$ ; in particular, the number of roots of  $f$  modulo  $p$  equals the number of fixed points of the Frobenius permutation.*

*Remark 4.2.* Theorem 4.1 gives a density among primes ordered by size, whereas A399163 is indexed by  $n$ . The two notions agree directly: the primes

$p_1, \dots, p_N$  are exactly the primes at most  $p_N$ , and  $N = \pi(p_N)$ . Thus, for any property  $S$  of primes,

$$\frac{\#\{n \leq N : p_n \in S\}}{N} = \frac{\#\{p \leq p_N : p \in S\}}{\pi(p_N)}.$$

As  $N \rightarrow \infty$ ,  $p_N \rightarrow \infty$ , so the limiting density is the same whenever the prime density exists. No use of the prime number theorem is needed for this equivalence.

Applying Chebotarev with  $G = S_6$ , the density of primes for which  $H$  has exactly  $k$  roots modulo  $p$  equals  $N_k/720$ , where  $N_k$  is the number of permutations of six letters with exactly  $k$  fixed points. The cycle-index formula gives Table 1.

TABLE 1. Elements of  $S_6$  by number of fixed points, and the resulting densities.

| $k$ (fixed points) | cycle types                    | $N_k$ | $N_k/720$ |
|--------------------|--------------------------------|-------|-----------|
| 0                  | (6), (4, 2), (3, 3), (2, 2, 2) | 265   | 53/144    |
| 1                  | (5, 1), (3, 2, 1)              | 264   | 11/30     |
| 2                  | (4, 1, 1), (2, 2, 1, 1)        | 135   | 3/16      |
| 3                  | (3, 1, 1, 1)                   | 40    | 1/18      |
| 4                  | (2, 1, 1, 1, 1)                | 15    | 1/48      |
| 5                  | —                              | 0     | 0         |
| 6                  | (1, 1, 1, 1, 1, 1)             | 1     | 1/720     |

Since  $265 + 264 + 135 + 40 + 15 + 0 + 1 = 720$ , these densities sum to 1.

## 5. THE EXCLUDED VALUE: WHY 5 NEVER OCCURS

**Corollary 5.1.** *For every prime  $p$ ,  $H$  has 0, 1, 2, 3, 4, or 6 roots modulo  $p$ , but never exactly 5.*

*Proof.* A permutation of a six-element set that fixes exactly five points must also fix the sixth point, so no element of  $S_6$  has exactly five fixed points. For unramified primes, the number of roots of  $H$  modulo  $p$  is the number of fixed points of a Frobenius element in  $G = S_6$ , so it cannot be 5. The only possible ramified primes are 2 and 743, and these were checked directly above; they give 0 and 1 distinct roots, respectively. Hence no prime gives 5 roots.  $\square$

Thus  $a(n) \neq 5$  for every  $n$ .

## 6. NUMERICAL VERIFICATION

We computed  $a(n)$  directly by factoring  $H$  modulo  $p_n$  in SymPy [2] for the first 20,000 primes, with  $p_n \leq 224,737$ . The first 88 computed values agree term for term with the published data for A399163 [5].

The observed counts and theoretical expectations are shown in Table 2. The chi-square goodness-of-fit statistic, using the six positive-probability categories, is  $\chi^2 = 3.87$  on 5 degrees of freedom, corresponding to  $p \approx 0.57$ .

TABLE 2. Observed versus expected counts among the first 20,000 primes.

| $k$ | observed | expected ( $20,000 \cdot N_k/720$ ) |
|-----|----------|-------------------------------------|
| 0   | 7378     | 7361.11                             |
| 1   | 7349     | 7333.33                             |
| 2   | 3731     | 3750.00                             |
| 3   | 1134     | 1111.11                             |
| 4   | 380      | 416.67                              |
| 5   | 0        | 0                                   |
| 6   | 28       | 27.78                               |

The value 6 occurs 28 times among the first 20,000 primes, with first occurrence at  $n = 1883$ , where  $p_{1883} = 16193$ .

## 7. CONCLUDING REMARKS

We determined the Galois group of the primitive sextic Misiurewicz polynomial  $H(x) = x^6 + 2x^5 + 2x^4 + 2x^3 + x^2 + 1$  to be  $S_6$ . Chebotarev's theorem then gives the exact limiting frequencies of its root counts modulo primes and explains, in particular, the absence of the value 5. It would be of interest to determine whether analogous Galois-group and density results hold for primitive Misiurewicz polynomials attached to other small pairs  $(m, k)$ ; we do not pursue this here.

## ACKNOWLEDGMENTS

Computations in this note — the discriminant, the modular factorizations, and the finite-field irreducibility certificates of Section 2 — were performed with the SymPy computer algebra system [2], and the Galois-group computation of Section 3 was cross-checked the same way.

## REFERENCES

- [1] H. W. Lenstra, Jr. and P. Stevenhagen, *Chebotarëv and his density theorem*, Math. Intelligencer **18** (1996), no. 2, 26–37.
- [2] A. Meurer et al., *SymPy: symbolic computing in Python*, PeerJ Comput. Sci. **3** (2017), e103.
- [3] J. Milnor, *Dynamics in One Complex Variable*, 3rd ed., Annals of Mathematics Studies, vol. 160, Princeton University Press, 2006.
- [4] J. Neukirch, *Algebraic Number Theory*, Grundlehren der mathematischen Wissenschaften, vol. 322, Springer, Berlin, 1999.
- [5] OEIS Foundation Inc., *The On-Line Encyclopedia of Integer Sequences*, Sequence A399163, <https://oeis.org/A399163>.