MATH 319NT

Computational Evidence for Dynamically Irreducibility of Certain Quintics over Finite Fields

Autumn Nguyen (*ngoc54n@mtholyoke.edu*), Mount Holyoke College

Abstract

Finding conditions to guarantee that a polynomial is **dynamically irreducible** (**DI**) has important implications in fields like arithmetic dynamics and cryptography. However, this is still an area of open research, with lots of unknowns around quintics. Through computational experiments in Magma for quintics of the form $x^5 + ax + b$, we discovered that there are **no DI quintics** in the finite field $\mathbf{F}_7$ and $\mathbf{F}_{43}$, and that there are **six potential DI quintics** in $\mathbf{F}_{11}$. Together with conjectures from patterns in critical orbits, our results provide grounds for discovering sufficient conditions to guarantee DI quintics in those finite fields.

Background

A polynomial $f(x)$ is **dynamically irreducible** (**DI**) if

$f^n(x) = (\underbrace{f \circ f \circ \ldots \circ f}_{n \text{ times}})(x)$ is irreducible **for all** n.

Here we are considering $f \in \mathbf{F}_p[x]$ of degree ≥ 2.

A **critical point** of $f(x)$ is a root of the derivative of $f(x)$. A **critical orbit** is the set of values generated by iterating $f(x)$ starting from its critical points.

For example, c is a critical point if $f'(c) = 0$. The sequence $\{c,\ f(c),\ f(f(c)),\ f(f(f(c))), \ldots\}$ forms the critical orbit of $f(x)$. Since the field is finite, this sequence eventually becomes periodic.

Results

The tables below show the quintics that stay irreducible after i$^{\text{th}}$ iterates in different finite fields.

Table 1: Finite field $\mathbf{F}_7$

1	12 quintics (out of 49 distinct ones in F_7)
2	2 quintics: $x^5 + x + 3$, $x^5 + x + 4$
3	None

Table 2: Finite field $\mathbf{F}_{11}$

1	18 quintics (out of 121)
2	10 quintics
3	6 quintics: $x^5 + 3$, $x^5 + 4$, $x^5 + 5$, $x^5 + 6$, $x^5 + 7$, $x^5 + 8$
4	The same six quintics above
5	The same six quintics above
>5	Not computed yet

Table 3: Finite field $\mathbf{F}_{43}$

1	336 quintics (out of 1849)
2	72 quintics
3	6 quintics: $x^5 + 3x + 10$, $x^5 + 3x + 33$, $x^5 + 6x + 11$, $x^5 + 6x + 32$, $x^5 + 25x + 15$, $x^5 + 25x + 28$
4	The same six quintics above
5	None

Methods

Scan to see the **code** for all computations!

Results (cont.)

From Table 1, there are no DI quintics in $\mathbf{F}_7$.
From Table 2, there are six potentially DI quintics in $\mathbf{F}_{11}$.
From Table 3, there are no DI quintics in $\mathbf{F}_{43}$.

In $\mathbf{F}_7$:
The two quintics irreducible after the 2nd iterate:

- $x^5 + x + 3$ has 2 critical orbits: $\{4,2,2\ldots\}$ and $\{2,2,2\ldots\}$.
- $x^5 + x + 4$ has 2 critical orbits: $\{3,5,5\ldots\}$ and $\{5,5,5\ldots\}$.

A quintic irreducible after 1st iterate (but reducible after 2nd iterate), $x^5 + 2x + 2$, has 2 critical orbits: $\{5,1,5,1\ldots\}$ and $\{6,6,6\ldots\}$.

A quintic reducible as it is, $x^5 + x + 2$, has 2 critical orbits: $\{1,4,1,4\ldots\}$ and $\{3,3,3\ldots\}$.

Discussion

For all of the quintics observed above, one orbit, out of the total of two, is a **constant value repeating**. The two quintics that stay irreducible after the 2nd iterate have their other orbits stabilizing as a constant value after the first element, such as $\{4,2,2,2\ldots\}$. The remaining quintics have their other orbits being a cycle of two elements, such as $\{5,1,5,1\ldots\}$.

It is therefore a possible conjecture that the quintics that stay irreducible for the longest number of iterates in $\mathbf{F}_7$ have one critical orbit that stabilizes as a constant value after the first element, while the remaining quintics have critical orbits being cycles of two repeated elements.

Thus, a suggestion for future research suggestion is to check if those patterns also hold for quintics in $\mathbf{F}_{11}$ and $\mathbf{F}_{43}$. Another future step is to compute further iterates of the six potentially DI quintics in $\mathbf{F}_{11}$ to increase our certainty.